universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

International Study: State of the Art of Electronic Signatures - Evaluation in 44 Nations

Verfasserin

Carina Isabella Freudenthaler

angestrebter akademischer Grad

Magistra (Mag. rer. soc. oec.)

St. Pölten, im November 2008

Studienkennzahl lt. Studienblatt: A 157

Studienrichung lt. Studienblatt: Diplomstudium Internationale Betriebswirtschaft UniStG

Betreuerin: ao.Univ.-Prof.Dr. Christine Strauß

Sperrvermerk

Die Diplomarbeit wurde im Rahmen eines Projektes des Forschungsvereines EC3 - E-Commerce Competence Center in Wien von mir erstellt. Die in der Arbeit enthaltenen Daten und Informationen stellen einen Wert da und sind wettbewerbsrelevant. Daher wird seitens EC3 gebeten, die enthaltenen Informationen unter Verschluss zu halten und die Arbeit auf 3 Jahre zu sperren und erst danach zu veröffentlichen.

Veröffentlichung, Vervielfältigung und Einsichtnahme sind ohne ausdrückliche Genehmigung der Firma E-Commerce Competence Center und des Verfassers bis zum 1.November 2011 nicht gestattet.

St. Pölten, 1. November 2008

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides Statt, die vorliegende Arbeit eigenständig und nur unter Verwendung der angegebenen Hilfsmittel angefertigt zu haben.

Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

St. Pölten, 1.November 2008

_____

Danksagung

An dieser Stelle möchte ich all jenen danken, die mich während meines Studiums begleitet haben und durch ihre fachliche und persönliche Unterstützung zum Gelingen der vorliegenden Diplomarbeit beigetragen haben.

Besonderer Dank gebührt Frau ao. Univ.-Prof. Dr. Christine Strauß für die Betreuung meiner Diplomarbeit und der wissenschaftlichen Unterstützung sowie der steten Förderung während meiner Studienlaufbahn. Sie ermöglichte es, meine Arbeit innerhalb der Forschungsgruppe „Digital Business Research, Development und Innovation Management (dBiz)“ des industriellen Kompetenzzentrums „EC3 -E-Commerce Competence Center“ anzufertigen.

Weiters möchte ich mich bei Herrn ao. Univ.-Prof. Dr. Karl Anton Fröschl bedanken, unter seiner wissenschaftlichen Leitung gearbeitet haben zu dürfen.

Ich bedanke mich bei meinem Freund Martin Blaha für seine alltägliche Unterstützung und seine große Geduld während der gesamten Studienlaufzeit, besonders aber in der Diplomphase.

Im Besonderen möchte ich meiner Mutter und meiner Großmutter danken, die mir dieses Studium durch ihre fortwährende Unterstützung überhaupt ermöglicht haben und mir stets Liebe und moralischen Beistand entgegengebracht haben.

Ich möchte diese Arbeit meinem Dad, Ing. Hannes Schneider, widmen, der 2002 von uns gegangen ist und furchtbar stolz auf mich wäre.

Danke!

Preface

In eCommerce, contracting partners have to identify each other and a valid declaration of intention has to be executed on either side. Therefore it is necessary to give great attention to the topic of internet security and safety. In this connection, I dealt with the realization of secure transaction and contract signing via the Internet and came across the subject of digital signatures as they are an integral part of each digital transaction.

As also businesses, particularly operating in the eCommerce and eBusiness sector, are dealing with the topic of secure business transactions, the study was compiled within the scope of a project at the research association E-Commerce Competence Center in Vienna. Within this cooperation with EC3 I was enabled to exhaust synergies and establish an international network of correspondences. At this point it should be noted that I hold the sole authorship of this study.

One project in the range of digital signature deals with the transnational application of digital signature, covering the European borders. On the basis of a first research, it became obvious that a global synopsis is nonexistent on European level. Thus, I have bothered compiling a structured synopsis in three dimensions: legal framework, technical standards and market penetration.

In this context, the following countries have been surveyed (table 1):

Table 1: surveyed countries, source: own illustration

EU members		
Austria	Germany	Netherlands
Belgium	Greece	Poland
Bulgaria	Hungary	Portugal
Cyprus	Ireland	Romania
Czech Republic	Italy	Slovakia
Denmark	Latvia	Slovenia
Estonia	Lithuania	Spain
Finland	Luxembourg	Sweden
France	Malta	United Kingdom
EU member candidates		
Croatia	Republic of Macedonia	Turkey

Other European countries		
Albania	Iceland	Russia
Armenia	Moldavia	Serbia
Azerbaijan	Monaco	Switzerland
Bosnia Herzegovina	Montenegro	Ukraine
Georgia	Norway	

To obtain a general idea about the current state in the country, an Internet research was started. Official State Websites, information sites of ministries of foreign and social affairs, and home-pages of IT and Telecom Agencies were called up, general information and contact addresses were collected.
For gathering detailed information, the chamber of commerce of each country has been contacted, either by email or by telephone, equally different governmental departments.
Furthermore, technical details were asked for by correspondence with different suppliers for Internet security and digital signature solutions.
A list of questions was prepared and sent out via e-mail. A huge range of e-mail contacts were established and around 22% responses on requests (of 661) were sent back from different companies and agencies.

It has to be mentioned, that the study is based on own findings and therefore can not bee esteemed to be exhaustive. Some of the informations given have not been published in journals or can not be found on websites but were provided by a huge range of correspondences.

The collected information was pulled together and compiled in the following study.
For purpose of clarity, the study is structured in-depth and subjective interpretations are left out to let the facts speak for themselves.
It cannot be ignored that a certain distortion of results can occur when regarding a county's profile. In some countries the collection of data was aggravated, often because of language barriers, and only few feasible data was available. This does not preclude that more data exists. This heterogeneity may incidentally further a somewhat false impression.

To gain a fast overview, a table on the end of each country analysis sums up the countries development concerning electronic signature standards and rating them in regard of available information and development in different categories.
The Rating is illustrated by using two types of valuation, shown in the following two tables:

a) color
The color indicates, how much information material has been found for that country and how many information has been obtained by building up correspondences (table 2).

Table 2: Meaning of colors, source: own illustration

colour	meaning
	a lot of information was available
	some information was available
	little information was available

b) letters

The Rating has been resolved by three ranks: AAA

The first position (fist A) stands for the legal framework, the second for the technical standard of electronic signature and the third position denotes the distribution of electronic signature.

To express the status of each country, the letters A, B and C are used (figure 1).

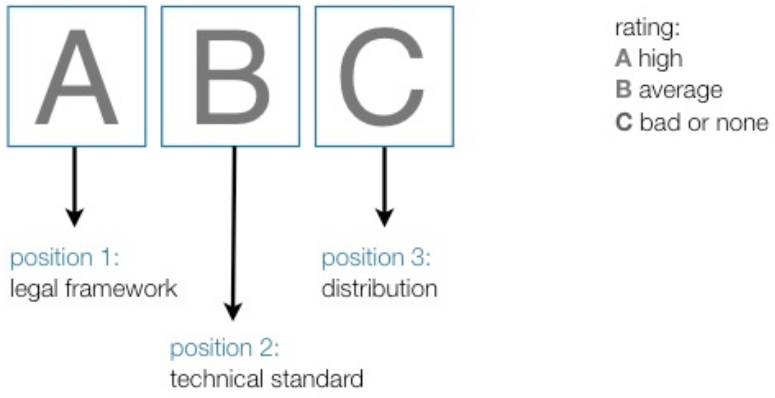


Figure 1: Explanation of rating, source: own illustration

AAA indicates, that this country has a funded legal framework, high-developed technical standards and a high distribution rate of electronic signatures.

CCC notifies that the country is in bad condition, both legally, technically and concerning distribution of electronic signature.

If only less or inadequate information could be found so that no statement concerning the development status or state of use can be given, this will be indicated by the additional character "-".

In a short summary at the end of the study, the countries are again listed up and their development is shown according to the structural setup chosen throughout the e survey, in combination with their respective rating.

The completeness of collected data is reflected in the country classification. EU member states have undertaken greater efforts to implement digital signature applications than non-EU members. In some countries no adequate information could be found to give a statement concerning certain issues. However, those sub-chapters are mentioned but kept empty to indicate the absence of information while simultaneously preserve unification of each country. Despite of great efforts to fill the gaps in those countries, where information was rare, the research was labored and outcome was partly unsatisfying. The effort was intensified but not accompanied by pursuant empiric results.

Index of contents

Appendices C to F are not in the print edition of this study but can be found on the attached CD-Rom.

List of Tables

List of Figures

List of Abbreviations

Abbreviation	Stands for
B2B	Business to business
B2C	Business to consumer
CA	Certification Authority
CA/CSP	Certification Authority / Certificate Service Provider
CRL	Certificate Revocation List
CSP	Certificate Service Provider
eID	electronic identity
EU	European Union
ICT	Information and Communication Technologies
KET	Key English Test
LDAP	Lightweight Directory Access Protocol
n.a.	not available
OCSP	Online Certificate Status Protocol
PDF	Portable Document Format
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRC	Population Register Center
RRN	Recurrence Rate Number
SIM	Subscriber Identity Module
S/MIME	Secure Multipart Internet Mail Extensions
SSCD	Secure signature-creation device
USB	universal serial bus
xAdES	XML Advanced Electronic Signature

1. Introduction

Today, we live in an e-era: eBusiness, eCommerce, eBanking and so on. These are keywords you can't imagine society and economy without and they form our everyday life. Internet has created a possibility with lots of advantages but also disadvantages.

Over 250 million Europeans use the Internet regularly, 80% of them have broadband connection. In Europe, 60% of public services are available online.[1] Information and communication networks are of vital importance in our society, allowing citizens to communication with each other and with public and private authorities and institutions.

One challenge is the anonymity of users in the world wide web and often creates problems in the area of authentication and integrity.[2] Security of electronic transactions over the Internet is a crucial issue today. The share of transactions that are carried out in cyberspace is gradually increasing. An electronic form more and more substitutes the paper.

One barrier is that in eCommerce and eCommunication, you can't see your opponent and it is not possible to see a proof of his identity (like passport or identification card).[3] Thus, People who make transactions in the Internet need security and trust. Trust is a necessary enabling precondition for sensitive services on the web and regarded as high important issue.[4] To conclude a contract, a high security standard is necessary to ensure, that the consignor is really the consignor and data have not been changed afterwards.

To use and profit form advantages of electronic medias in these sensitive areas, electronic signatures have been developed.[5] To produce relief, electronic signature can be used when doing business on the Internet[6] so that data can be transferred in a secure way. Electronic signatures enable the guarantee of authenticity and integrity of electronic transmitted documents. The legal certainty and the authenticity of electronic signatures are anchored in the law.[7]

---

[1] cf. European Communities, EU: i2010 is starting to deliver, http://www.epractive.eu/document/4644, access on 2.10.2007, 09:33

[2] cf. Andersson, Helena, Bylund, Markus et al., Survey of Privacy and Information Technology, SAITS project, V.1.0

[3] cf. http://www.securityfocus.com/infocus/1756, access on 27.06.2007, 12:30

[4] cf. Andersson, Helena, Bylund, Markus et al., Survey of Privacy and Information Technology, SAITS project, V.1.0

[5] cf. Nuster, Michael, Spezifische Fragen im Zusammenhang mit elektronischen Signaturen, 2005, Artikel in It-law.at, http://www.it-law.at/index.php?id=25&tx_publications_pi1[id]=73&cHash=049365313a, access on 01.10.2007, 8:35

[6] cf. http://www.securityfocus.com/infocus/1756, access on 27.06.2007, 12:30

[7] cf. Nuster, Michael, Spezifische Fragen im Zusammenhang mit elektronischen Signaturen, 2005, Artikel in It-law.at, http://www.it-law.at/index.php?id=25&tx_publications_pi1[id]=73&cHash=049365313a, access on 01.10.2007, 8:35

1.1 The need for standardization

To ensure standardized norms, requirement applications for electronic signature, the European Commission and other institutions have started initiatives to harmonize regulations and systems. Some significant initiatives are described shortly below.

1.1.1 Common Criteria Recognition Agreement (CCRA)[8]

The Common Criteria Recognition Agreement is an international agreement to ensure that

- products are evaluated to determine the security properties
- supporting documents used within the certification process define how evaluation methods and criteria are applied
- the certification can be issued by certificate authorizing schemes and
- the certificates are recognizes by all signatories of the Agreement.

The Agreement is based on the Common Criteria for Information Technology Security Evaluation(CC) and the Common Methodology for INformation Technology Security Evaluation (CEM) and aims to widely recognize secure IT products.

The Agreement declares that assurance levels (EALs) that are defined between versions of the criteria are recognized equivalently and can be used without restrictions.

1.1.2 European Electronic Signature Standardization Initiative (EESSI)[9]

The European ICT Standards Board (ICTSB) together with the European Commission stated an initiative to bring the industry and public authorities together under the European Electronic Signature Standardization Initiative (EESSI). This initiative was supported to identify the needs for standardization activities.

1.1.3 eEurope Initiative[10]

The eEurope initiative was started to accelerate positive changes of Information Society in the European Union and bring benefits to all Europeans. Its aim is to bring all citizens, businesses and administration into the digital age, build trust and strengthens. Institutions that are involved in the standardization work to realize eEurope are CEN, CENELEC and ETSI, that gave extensive interest in developing the ICT field in the European Union.

---

[8] cf. Common Criteria, http://www.commoncriteriaportal.org, access on 01.10.2007, 8:42

[9] cf. Sealed, DLA Piper and Across communications, Study on the standardisation aspects of eSignature, final report, 22.11.2007

[10] cf. http://www.ictsb.org/Activities/Documents/eEurope_initiative.pdf, access on 01.10.2007, 10:24

1.1.4 ETSI[11]

The European Telecommunication Standard Institute was founded in 1988 by the European Commission to establish a european wide standard for the telecommunication sector in technical concerns. Among others, ETSI developed a standard for electronic signature.

1.1.5 CEN[12]

CEN is the European Committee for Standardization and produces a series of regulations concerning electronic signature issues. They relate to the standardization effort of the eEUrope initiative. Working groups formulate CEN Workshop Agreements, for example „Security requirements for Trustworthy Systems Managing Certificates for Electronic Signatures“, „Security requirements for signature creation applications“, „General guidelines for electronic signature verification“ etc.

1.1.6 CENELEC[13]

CENELEC is the European Committee for Electrotechnical Standardization. It was created in 1973 as a non-profit organization, set up under Belgian law, that was composed of Committees of 30 European Countries. CENELEC aims to harmonize standards and develop a single european market for electronic and electrical goods and services.

1.1.7 ICTSB [14]

The ICT Standard Board (ICTSB) is an initiative of CEN, Cenelec and ETSI to coordinate specification activities in the sector of Information and Communications Technologies.

1.2 Legal framework

1.2.1 The European Directive of December 13, 1999/93/EG for Electronic Signature

For the use of electronic signature, a legal framework must be given to ensure that the electronic declaration has also legal meaning and is valid before the court.[15]

---

[11] cf. http://www.etsi.org/WebSite/AboutETSI/AboutEtsi.aspx, access on 1.10.2007, 10:53

[12] see http://www.cen.eu,

[13] see. http://www.cenelec.eu

[14] see. http://www.ictsb.org/

[15] cf. http://www.internet4jurists.at, access on 10.06.2007, 13:51

Therefore, the European Union adopted a community framework for electronic signature that has been implemented in different various countries.[16] In all European member states, the directive had to be implemented in national law until the 19.07.2007.

Primarily, only the term digital signature was used, because it refers to the technical encryption procedure, the public key encryption. However, the European Directive for electronic signature chose to use the uniform formulation „electronic signature", to include other types of encryption that may be used in the future.

The basic principles of this directive include:[17]

- the legal recognition: If a certificate, the certification service provider and the signature product used meet specific requirements, the resulting electronic signature is hold valid and equal to handwritten signature and can not be legally discriminated or denied.
- free circulation: All electronic signature products can circulate freely.
- liability: The eSignature Directive contains minimum liability rules for certification service providers to be liable for the validity of the certificate. This legislation ensures a free movement of certificates and builds consumer trust. Operators are stimulated to develop secure systems.
- a technology-neutral framework: The legislation enables legal recognition of eSignatures independent from the technology used.
- no closed user groups: The legislation regulates the issuance of certificates and certification related services. It does permit the insertion of schemes of different systems where no regulations are needed and trust already exists.
- international dimension: The legislation also includes mechanisms for a cooperation with third countries. like mutual recognition of certificates and other agreements.

1.2.2 Agreement on mutual acceptance of foreign certificates

In March 1998, an agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:
Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.[18]

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:[19]

---

[16] cf. http://www.securityfocus.com/infocus/1756, access on 27.06.2007, 12:30

[17] cf. Sealed, DLA Piper and Across communications, Study on the standardisation aspects of eSignature, final report, 22.11.2007

[18] cf. Study of the Donau University Krems, Master-Study, Austria

[19] cf. Study of the Donau University Krems, Master-Study, Austria

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

1.3 Definition

Electronic signature is no synonym for digital signature, although these two terms cannot easily be distinct.

Digital signature is a subset of electronic signature; it is a precise type of it. In contrast to an electronic signature, a digital signature is a specific technology that is based on asymmetric encryption.[20] It is a unique numerical value based on the entire written document that is being signed[21] with the aim to secure the origin and the integrity of data.[22] Digital Signature uses digital technology for the generation of electronic signature. The electronic signature is the legal concept that refers to all kinds of data authentication[23] and can include a printed name, an e-mail address, and a scanned signature.[24]

The relationship is schematically represented in figure 2:

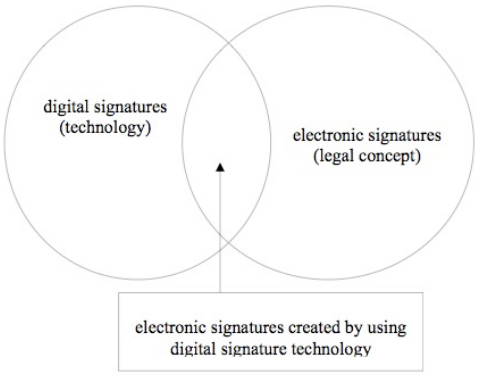


Figure 2: Relationship between „digital“ and „electronic“ signature, source: Dumortier, Jos, Legal Status of Qualified Electronic Signatures in Europe, in ISSE 2004-Securing Electronic Business Processes (2004)

[20] cf. Dumortier, Jos, Legal Status of Qualified Electronic Signatures in Europe, in ISSE 2004-Securing Electronic Business Processes (2004)

[21] see. http://www.out-law.com

[22] cf. Dumortier, Jos, Legal Status of Qualified Electronic Signatures in Europe, in ISSE 2004-Securing Electronic Business Processes (2004)

[23] cf. Dumortier, Jos, Legal Status of Qualified Electronic Signatures in Europe, in ISSE 2004-Securing Electronic Business Processes (2004)

[24] see. http://www.out-law.com

1.3.1 Types of electronic signature

This EU-directive on electronic Signature describes three types of electronic signature with different juridical value:

- electronic signature
- advanced electronic signature
- advanced electronic signature which is based on qualified certificate and which is created by a secure-signature-creation device.

1.3.2 Basic electronic signature

Paragraph 2 of the EU-directive defines basic electronic signature as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[25]

1.3.3 Advanced electronic signature

An advanced electronic signature (also secure signature) is only valid if it is compliant with some legal standardized regulations and must fulfill special requirements:

> “[a] it is uniquely linked to the signatory;
> [b] it is capable of identifying the signatory;
> [c] it is created using means that the signatory can maintain under his sole control;
> [d] it is linked to the data to which it relates that any subsequent change of the data is detectable".[26]

To sign documents, a special cryptographic procedure that is based on an asymmetric encryption is used.

1.3.4 Qualified electronic signature

This type of electronic signature is not explicitly defined in the European Directive as it corresponds to higher security requirements. The qualified electronic signature is an advanced electronic signature that is based on a qualified certificate and created by a secure signature creation device. To be classified as „qualified“ certificate, additional requirement must be met.[27]

According to the European Directive, only qualified certificates have the same legal value as handwritten signatures. [28]

---

[25] cf. EU-Directive on electronic signature n.93/199

[26] cf. EU-Directive on electronic signature n.93/199, art.2.2

[27] cf. Sealed, DLA Piper and Across communications, Study on the standardisation aspects of eSignature, final report, 22.11.2007

[28] cf. Sealed, DLA Piper and Across communications, Study on the standardisation aspects of eSignature, final report, 22.11.2007

1.4 The asymmetric public key encryption

The most significant kind of application of an electronic signature is the digital signature. A digital signature is based on the encryption of a document.

Therefore, the digital signature uses two keys. This pair consists of a private and a matching public key. This is called an asymmetric encryption or public-key-method. The private key is secret and not known, not even for the user. A password, a pin-code or a smart card secures this private key.

The public key is free available on the Internet and serves for verification of the signature. With help of mathematical procedures, an electronic fingerprint is created: the whole document comes under scrutiny and a so-called Hash is calculated from all characters and encrypted wit the private key. The document is transmitted electronically in line with the signature. The receiver can verify the public key via the Internet. Is it identical with the calculated one, the document relegated in the original state.[29]

An advanced electronic signature has great importance for all who must effect electronic transactions as they have a deep juridical value and can thus be used for high-value eCommerce businesses.
Figure 3 shows the mode of operation using electronic signature.

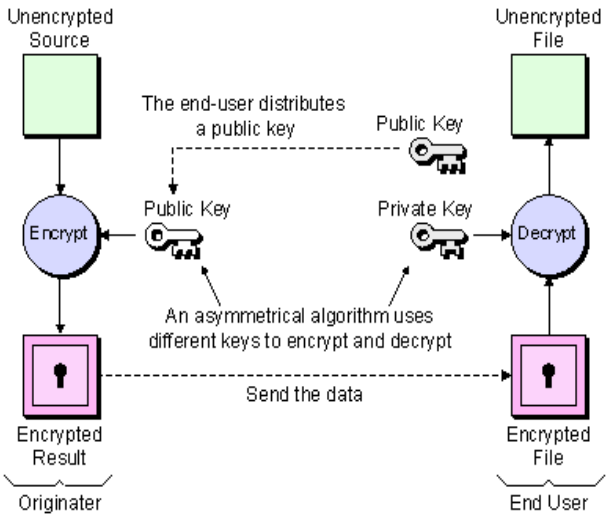


Figure 3: mode of operation, using digital signature,
source: http://www.chipdesignmag.com/display.php?articleId=1162, access on 10.06.07, 15:12

[29]cf. http://www.internet4jurists.at, access on 10.06.2007, 13:51

1.5 Certificates

To sign in a secure was, a qualified certificate is necessary, that is issued by a Certification Service Provider. A certificate binds your public key to your identity.[30]

The Certification Service Providers serve as „Trusted Third Party“ that is responsible for the correctness of the issued certificate. The certificate has to be conforming to the legal requirements for certificates and can only be issued for certain time.

To fulfill their functionality, certificates must contain the following minimal information:

- name of user
- public key of user
- electronic signature of the Certificate Service Provider.[31]

1.5.1 Certificate Service Provider

A Certification Authority certifies the keys. It guarantees the authenticity of the key and the observation of the policies.

1.5.2 The Certificate Revocation List (CRL)

But certificates are not trustable for hundred percent. A certificate can be stolen or compromised, turn invalid or be issued incorrectly. If such problems occur, a Certificate Revocation List or an Online Certificate Status protocol is provided.

The Certificate Revocation List contains all revoked certificates in line with the reason for revocation.

If someone wants to access a server, the CRL is checked for validity of the certificate and the access is granted or denied, belonging to the status of the certificate.

To be up-to-date, this list must be downloaded regularly.[32]

1.5.3 The Online Certificate Status Protocol (OCSP)

The Online Certificate Status Protocol was created alternatively to the CRL to overcome the limitation of the CRL that has to be downloaded to keep it current. The status of a certificate is checked in real time.[33]

---

[30] cf. http://www.out-law.com, access on 11.06.2007, 09:12

[31] cf. Hauber, Julia, Faktische Probleme der elektronischen Signatur, Seminararbeit, WU Wien, 2003

[32] cf. http://www.searchsecurity.com, access on 10.06.2007, 14:32

[33] cf. http://www.searchsecurity.com, access on 10.06.2007, 14:02

1.6 Electronic Signature Products

An Electronic Signature Product is a hard or software, which is used by a CSP for the supply of electronic signature services. It is also used for creation and verification of an electronic signature.

1.6.1 eSignature mediums

A lot of enterprises developed and provide signature software to create electronic signatures for special purposes to enable security, efficiency and cost-effectiveness.

XML Signing solution

XML makes the use of PKI signatures possible for a range of applications. A XML signed document can be transferred between systems, the signature can be verified by any system as well as the integrity and non-repudiability.[34]

The enterprise E-Lock provides a range of signature solutions. For XML format, E-Lock offers X-Web Form Manager that enables to gather information with forms and process it via a customizable workflow. The forms are created with an XML editor and are fully customizable. Each Phase of the procedure can be secured by digital signatures.
Another solution is the X-Digital Signature Suite that provides digital signature technologies and non-repudiation. Any data can be represented in XML format and digitally singed. This product uses certificates on smart cards, USB tokens or certificates stored on the workstation.[35]
More information about E-Lock can be found on the website http://www.elock.com.

PDF, PDF/A and digital signature

PDF (Portable Document Format) is an overall file format for printable documents that was developed by Adobe Systems and published in 1993. It is a wide used and recognized standard for the exchange and also for storage and archiving of electronic documents worldwide.[36]

PDF/A is a standard that was developed by different industries and enterprises around the world. It is a file format that is based on PDF that provides a mechanism to display electronic documents so that the visual appearance is conserved over time, independent of tools and systems of creation, storage or reproduction.[37]

---

[34] cf. E-Lock, XML Signing Solution, http://www.elock.com/xml-signing.html, access on 1.10.2007, 12:23

[35] cf. E-Lock, XML Signing Solution, http://www.elock.com/xml-signing.html, access on 1.10.2007, 12:23

[36] cf. PDF Sigantur, Signatur und PDF/A, http://www.pdf-signatur.at/signatur-und-pdfa.html, access on 1.10.2007. 13:12

[37] cf. PDF Sigantur, Signatur und PDF/A, http://www.pdf-signatur.at/signatur-und-pdfa.html, access on 1.10.2007. 13:12

The PDF format allows the inclusion of different electronic signatures, PDF/A accepts the document signature.[38]

Adobe for example generate MDP (Manipulation Detection and Prevention) signatures and UR (Usage Rights) Signatures.[39] For more information about Adobe Security Solutions see http://www.adobe.com/de/security/index.html.

The Signatures can either be

- invisible: don‘t modify the appearance of the document or
- visible: the existence of the signature is indicated by a separate display within the document.[40]

The enterprise OpenLimit offers a Plug-in for Adobe Reader / Acrobat to sign PDF files. For example with the OPENLIMIT SignCubes printer diver the user can generate a TIFF, PDF and PDF/A file form any application. This client application generates certified and advanced eSignatures that are legal binding.[41]

The Open-Source office package OpenOffice is now available in the new version 2.4 for Windows, Linux and Solaris for download. In this new version, documents can be stored in the PDF/A standard for long time archiving.[42]

S/MIME and OpenPGP

S/MIME means Secure/Mulipurpose Internet Mail Extension and is an encrypting and signature standard for MIME capsuled Emails. This method serves for asymmetric encryption of eMails via authentication and for digital signatures using PKCS specifications. S/MIME accepts digital certificates according to X-509 standards. S/MIME is supported by most mail clients.
Alternatively, the user can also apply OpenPGP using PKI.

1.6.2 Signature-Creation Devices

To create an electronic signature, a signature-creation device is used. It is a system that is based on an encrypting and a decrypting algorithm with associated encryption keys. This device can either be software-based (typically contained in electronic mail systems) or hardware-based (when the signature-creation data is stored on a chip card).

Examples for signature-creation devices are smart cards, smart pens, mobile phones, PDAs or computer hard disks.

---

[38] cf. PDF Sigantur, Signatur und PDF/A, http://www.pdf-signatur.at/signatur-und-pdfa.html, access on 1.10.2007. 13:12

[39] cf. PDF Sigantur, Signatur und PDF/A, http://www.pdf-signatur.at/signatur-und-pdfa.html, access on 1.10.2007. 13:12

[40] cf. PDF Sigantur, Signatur und PDF/A, http://www.pdf-signatur.at/signatur-und-pdfa.html, access on 1.10.2007. 13:12

[41] cf. OpenLimit, OpenLimit CC Sign 2.1.6.3, https://www.openlimit.com/EN_PROD-OPENLiMiT-CC-Sign.html, access on 1.10.2007, 12:59

[42] cf. Heise Online, Feinschliff für OpenOffice, press release, 27.3.2008, http://www.heise.de/newsticker/Feinschliff-fuer-OpenOffice--/meldung/105557, access on 27.03.2008, 15:38

•eID card:
Many countries have developed electronic identity cards that store electronic certificates for authentication and electronic signature.

•Electronic signatures and credit cards:
Credit cards gain worldwide acceptance. But the threat of misusage of the credit card data is always given.
Some credit cards can be provided with a digital signature function and a lot of applications can be accessed in a secure way, like eProcurement, eGovernment, eBanking, eTax etc.
By using electronic signature, an exact allocation of the card holder is possible. Furthermore, the signature can be documented objective and unsophisticated by time stamping the transaction.

1.6.3 Card readers

To be able to read out the signature-creation data from a smart card, a card reader is required.

But there are several types of card readers, which can be differentiated as follows:

- Simple `transparent` card reader: Has no keypad or screen, just reads the card (for example eID card), to make it compatible with the ID card, no modification is required, just has to fulfill the Personal Computer/Smart-Card standard
- Card reader with built-in keypad/screen: card reader with secure pin-pad (keypad to enter pin-code securely), modification necessary to receive Pin-codes and display messages on screen.
- Card reader for PC Card slot: can be fully integrated into computer
- Keyboard that incorporates a card reader: this is an ordinary card reader that is fitted into keyboard housing.
- Card readers that are built in computers as a standard.

Card readers are divided into different security categories (table 3):

Table 3: Classification of card readers, source: http://www.computeruniverse.net/tips/kartenleser.asp, access on 11.06.2007, 21:39

Classes	Specifications
Class 1	doesn't offer security, as it just contacts the card and reads or write it
Class 2	must not transfer the PIN to the computer, number has to be saved in the card reader
Class 3	a display is necessary, that shows the whole transaction, user can control the whole process.
Class 4	highest security level, have their own identity, provided with a signature key, can create their own digital signature

1.7 Public Key Infrastructure (PKI)

The Public Key Infrastructure can be implemented to enable computers to authenticate each other. This infrastructure enables to use the public key information that is contained in the public key certificate so that messages can be encrypted. Confidentially is establishes and message integrity and user authentication verified.[43]

By the use of public and private cryptographic key pair, shared through a trusted authority, data can be securely and privately exchanged.

A public key infrastructure consists of:

- A certificate authority that issues and verifies the digital certificate
- A registration authority that acts as the verifier for the certificate authority
- A directory where the certificates (with their public keys) are held and
- A certificate management system.[44]

Both, the CRL and the OCSP, are common methods when a PKI is existent to maintain access to a server.

1.8 Electronic signature related applications

There are a wide range of applications that require electronic signature. Areas for the use of qualified electronic signatures include eGovernment services, document signing, eInvoicing, public eProcurement and eAdministration services.[45]

In the public sector, most member states make use of electronic signatures. In some countries the communication with public authorities is only possible by using electronic signatures.[46] Citizens have to identify themselves to benefit from a a huge range of public online services.

1.8.1 eGovernment

The term eGovernment comes from electronic government and refers to the use of a platform to exchange information, provide services and transact with citizens or businesses.

---

[43] cf.: http://mcwg.org/mcg-mirror/cert.htm, access on 10.06.2007, 13:57

[44] cf.; http://www.searchsecurity.com, access on 10.06.2007, 14:02

[45] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[46] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

eGovernment can improve the internal efficiency or processes of governance like Government-Government (G2G) and Government-to-Employees (G2E) models, other models are Government-to-Citizen and Government-to-Customer (G2C) and Government-to-Business (G2B) models.[47]

The main activities of eGovernment are publishing information online, enabling a two-way communication between government agencies and citizens, businesses or other government agencies, conducting transaction and governance.[48]

Most Public Administration Authorities offer information online and switch over to offer all transaction concerning official procedures online. Forms must no longer be downloaded but can be filled, signed and sent electronically.

eGovernment includes all procedures, from filing an proposal to execution of an application:[49]

- Internet portal: Information about official channels
- Specific application: electronic handling of procedures
- dual delivery: electronic delivery of post.

Notifications and other documents must not be delivered via post but can also be transmitted electronically.[50]

The range of services offered can be divided into several domains, like eVoting, eAdministration, eDEmocracy and more. Under the subarea eAdministration the offer of electronic forms, electronic tax declarations, electronic building applications etc can be classified.[51]

The integration of electronic signature provides information and data security at the highest stage. User IDs and passwords that have to be managed will be a thing of the past. By using electronic signatures the processing of electronic procedures will be facilitated and data protection and privacy will be significantly secured.[52]

Benefits of eGovernment include improvement of efficiency, convenience and accessibility of public services.[53]

---

[47] cf. IT Wissen, eGovernment, http://www.itwissen.info/definition/lexikon, access on 1.10.2007, 11:14

[48] cf. IT Wissen, eGovernment, http://www.itwissen.info/definition/lexikon, access on 1.10.2007, 11:14

[49] cf. Digitales Österreich, Was ist E-Government?, http://www.digitales.oesterreich.gv.at/site/5230/default.aspx, access on 01.10.2007, 11:16

[50] cf. Digitales Österreich, Was ist E-Government?, http://www.digitales.oesterreich.gv.at/site/5230/default.aspx, access on 01.10.2007, 11:16

[51] cf. IT Wissen, eGovernment, http://www.itwissen.info/definition/lexikon, access on 1.10.2007, 11:14

[52] cf. Digitales Österreich, Was ist E-Government? - Electronische Amtswege, http://www.digitales.österreich.gv.at/site/5619/default.aspx, access on 01.10.2007, 11:16

[53] cf. Digitales Österreich, Was ist E-Government?, http://www.digitales.oesterreich.gv.at/site/5230/default.aspx, access on 1.10.2007, 11:16

Electronic Voting

Electronic Voting is used for many and divers processes in the public area. The term indicates the use of electronic media for obtaining respectively advancing an opinion.
One part is application of electronic voting for evaluation and transmission of electronic results.[54]

An electronic system for vote must fulfill certain requirements:

- Only eligible voters are allowed to vote.
- Counting must be correct and confirmable.
- Votes must be anonymous.
- The voters must be authenticates to prohibit the sale of votes.[55]

eVoting systems must ensure the definite identification of the voter and the anonymity of his voting decision. The authentication can be resolved by using digital signature, but also by password authentication, cryptocards or electronic fingerprinting.[56]

In some countries it is already possible to contest an election electronically.

eProcurement

To be compliant with the European Directive, both applications must rely on advanced electronic signatures.[57]

eProcurement terms procurement by electronic means. Public eProcurement means eProcurement in the public sectors. eProcurement can improve and simplify government procurement operations. Enterprises can identify contract opportunities and supply goods and service across national borders in the European Market. Thereby, Europe gains competitiveness and economic growth.[58]

The European Commission promotes the use of eProcurement by creating awareness of benefits and opportunities of transborder eProcurement and provides functional requirements, fools or services for contracting authorities to facilitate electronic public procurement.[59]

eProcurement include many market procedures, like eTendering, ePublication, eAwarding, eNegotiation, eContracting, eInvoicing and more.[60]

---

[54] cf. Arbeitsgruppe E-Voting im BMI, Unterarbeitsgruppe Internationales, Bericht (T.M. Buchsbaum), 20.10.2004

[55] cf. Andersson, Helena, Bylund, Markus et al., Survey of Privacy and Information Technology, SAITS project, V.1.0

[56] cf. IT Wissen, eGovernment, http://www.itwissen.info/definition/lexikon, access on 1.10.2007, 11:14

[57] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[58] cf. European Commission, eProcurement, http://ec.europa.eu/idabc/en/document/2084/5874, access on 1.10.2007, 9:12

[59] cf. European Commission, eProcurement, http://ec.europa.eu/idabc/en/document/2084/5874, access on 1.10.2007, 9:12

[60] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

By trading across borders and purchasing goods and services electronically, all sectors including public administration, businesses and citizens will benefit.[61]

Electronic Tax declaration

A lot of governments provide electronic tax systems to its citizens and businesses. Legal or natural persons can submit their tax declarations by filling in an online form, sign it and send it to the local Tax Administration electronically.

1.8.2 eBanking

eBanking means electronic banking or online banking and covers all electronic bank operations between client and credit institution. Online Banking uses electronic communication technologies and networks and requires a connection to the Internet. It can be administrated by personal identification number (PIN) and transaction number (TAN). This PIN/TAN procedure is the standard for financial transactions, but some banks have already adopted an electronic signature application for securing the transaction without using PIN/TAN mode. [62]

1.8.3 eHealth

Also for the health sector, state-of-the-art information and communication technologies are used by providing health tools for healthcare professionals or patients and offering a range of services for health via Internet.

eHealth covers interactions between health service providers and patients, transmission of data between institutions or peer-to-peer communication between health professionals and patients. For this occasion, health information networks, telemedicine services, health portals and many other tools are provided.

These eHealth systems provide patients with actual information and simplifies the access and sharing of information between healthcare professionals.

Building healthcare systems is a national responsibility and national authorities are main players in the European Union. The European Commission helped national organizations to learn form each other and facilitates the development across the European Union.

---

[61] cf. European Commission, eProcurement, http://ec.europa.eu/idabc/en/document/2084/5874, access on 1.10.2007, 9:12

[62] cf. IT Wissen, eGovernment, http://www.itwissen.info/definition/lexikon, access on 1.10.2007, 11:14

1.9 Benefits and barriers of electronic signature

1.9.1 Identity[63]

Identity is the definite identifier for a person, an organization resource or service in combination with optional additional information (like authorization, attributes). There are several techniques for identity marks like the ID number or electronic key, that ensures the identity of the user, as well as diverse methods to proof and determine identity.

1.9.2 Authentication

Digital signatures are used to authenticate the source of a message. A valid signature indicates that the massage was sent by the user, the secret key is bound to. Especially for financial transaction a high confidence in the sender‘s authenticity is evident.

1.9.3 Integrity

There is also the need for confidence that a message has not been modified during transmission. Encryption hides the content and the digital signature secures the integrity of the message. if the content was altered somehow, the signature will be invalid.

1.9.4 Secure electronic transactions

The use of electronic signature secures electronic transaction and communication in the Internet, especially in the following areas:

•eCommerce:

Online Commerce is insecure and transactions often make detour. Each connection runs over about 10 nodal pints and the threat of manipulation and read along occurs.

•eBanking:

For example applications for electronic signatures can protect against Trojans, viruses and phishing at eBanking processes.

A lot of banks insert digital signatures for secure their Online-banking application.

With so called phishing attacks, the user of online banking systems is persuaded to notify one or more TANs by using pretended motivations. By applying electronic signatures, users can be protected from such offenses. The user enters a PIN to compile a transaction and uses his chip card to effect the electronic signature.

Also the data of the bank account can be manipulated during the eBanking application. The use of

[63] cf. IT Wissen, eGovernment, http://www.itwissen.info/definition/lexikon, access on 1.10.2007, 11:14

electronic signature prevents such misusage through the function of seals. A change of data is impossible because of the hash function.[64]

•Advantages for retailer:
In online shops, customers can order different products and services. But in every eShop, also incorrect and invalid orders are sent, that cause high additional costs for the retailer, like for back postings etc. Also indication of false address or credit card data can lead to suspension of payments.
By applying an electronic signature application, authenticity of the order can be guaranteed.

1.9.5 reasons for using electronic signature

In November 2007, Sealed, DLA Piper and Across communications published a study on the standardization aspects of eSignature. For compiling the study, a lot of correspondences have been established, for example with certification services providers, public authorities or member states policy makers.
About 73% of responding institutions are using electronic signatures, 9% plan to implement them and 18% do not intend to provide and use electronic signatures.
Mostly, the country eGovernment applications use electronic signatures, followed by document signing. Services like eBanking, eInvoicing or eProcurement are offered.[65]

Figure 4 shows the purposes for using electronic signatures:

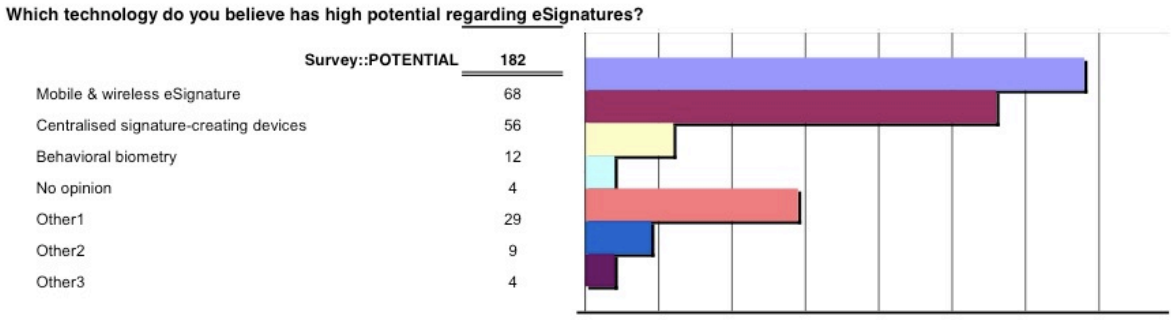


Figure 4: purposes for using or implementing eSignatures, source: Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

1.9.6 Barriers of electronic signatures

[64] cf. Transaktionssicherheit Sicherer Signaturen, V. 1.0, April 2006, http://www.a-trust.at/docs/Transaktionssicherheit_Sicherer_Signaturen.pdf access on 06.11.2007, 18:02

[65] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

Some institutions are not using electronic signature because their believe that there is no business need for it and it seems difficult to implement eSignature applications (figure 5).[66]

One big obstacle to the acceptance and proliferation of electronic signatures is the lack of interoperability of systems and applications, both national and cross border. For example, many applications only accept certificates form one certification authority.[67]

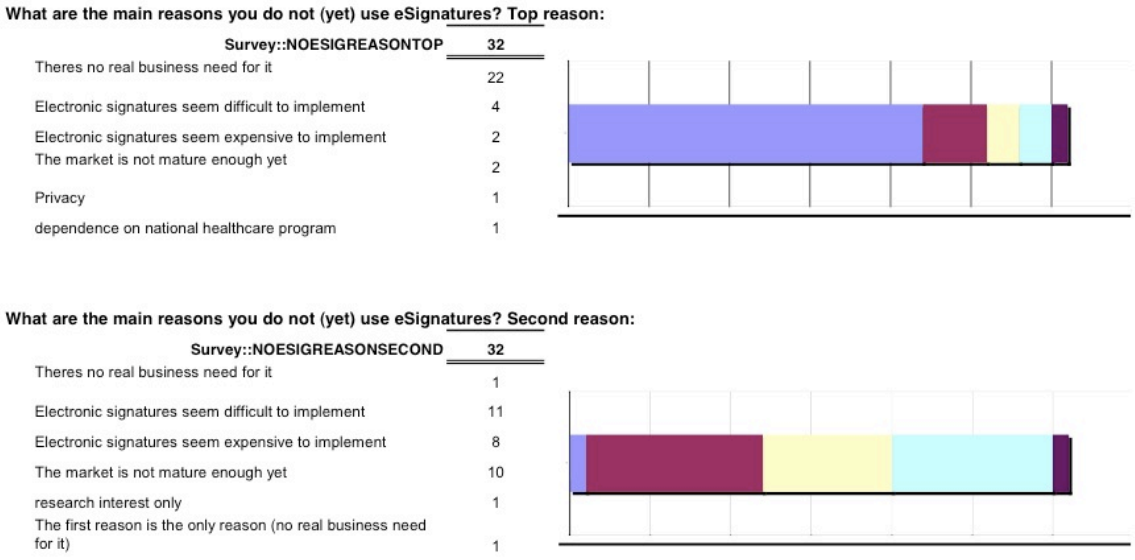


Figure 5: reasons for not using electronic signatures, source: Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

Evolaris sums critical factors of success and barriers of the use of electronic signatures in business area (figure 6). These have been determined by Evolaris acceptance monitor, that enables to measure and illustrates the specifications of relative advantage, compatibility, complexity etc. The characteristics are rated according to a scale form 1 to 5. The value 5 for the characteristics like relative advantage, compatibility means highly distinction and acceptance of technological innovations, for the characteristics complexity and perceived risk the value 5 means poor specification. [68]

[66] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[67] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[68] cf. Evolaris Solution Center, Akzeptanz elektronischer Signatur, Dezember 2003

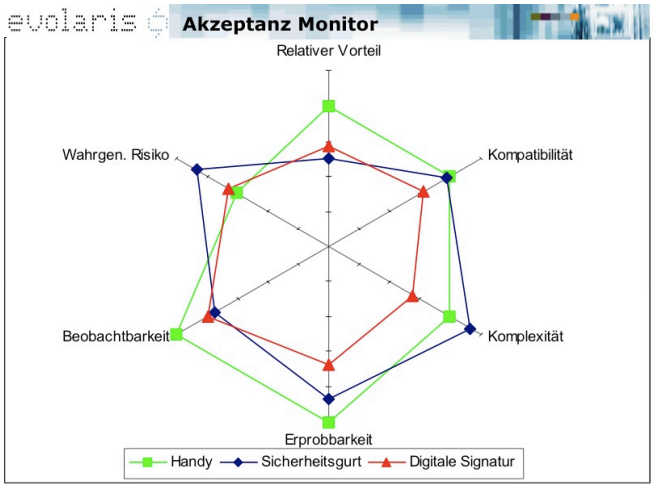


Figure 6: Acceptance Monitor, source: Evolaris Solution Center, Akzeptanz elektronischer Signatur, Dezember 2003

The interviews that are carried out for this demonstration devote the following use barriers:

- absent benefits / high costs
- perceived risk, lack of trust (technical problems, decline in prices)
- little compatibility and
- high complexity.[69]

1.10 eSignature initiatives

A lot of EU and non-EU initiatives have been started to support electronic Signatures and electronic signature operations.[70] Some significant initiatives are described shortly below.

1.10.1 European Commission initiatives

eEurope Initiative

In December 1999, the European Commission started the eEurope initiative to ensure benefits of an information society, bringing communities closer together, sharing knowledge and creating wealth.[71] The key objectives include:

[69] cf. Evolaris Solution Center, Akzeptanz elektronischer Signatur, Dezember 2003

[70] cf. Sealed, DLA Piper and Across communications, Study on the standardisation aspects of eSignature, final report, 22.11.2007

[71] cf. Panayiotou, Panayiotis Andrea, Electronic Governance for the Lands and Surveys Department in Cyprus, FIG Working Week 2004, AThens, Greece, May 22-17, 2004

- bring Europe into the digital age
- create a digitally-literate Europe
- ensures a process that is socially inclusive, building customer trust.[72]

IDABC related initiatives[73]

IDABC means Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens and is managed by the Directorate-General for Informatics of the European Commission. The program aims to improve collaboration and consequently efficiency between European public administration and encourages public sector services to businesses and citizens cross border in Europe. To make Europe an attractive place to work, invest and live, IDABC develops solutions, issues recommendations and provides services to enable national and cross border administrations to communicate electronically by using stat-of-the-art technologies. IDABC contributes to the i2010 initiative.

1.10.2 EU Projects

i2010 eGovernment Action Plan[74]

The Commission of the European Communities presented an eGovernment Action Plan as part of its i2010 initiative.

The i2010 initiative faces a lot of objectives including the creation of a single information space, providing benefit to all citizens from trusted innovative services, establishing transparency and accountability, allowing convenient, secure and interoperable authentication to access public services across Europe and making efficiency and effectiveness for all participants in Europe a reality by 2010.

eTen[75]

eTEN is a program of the European Community to provide the application and availability of electronic services in the European Union. In addition, the eTEN program should stimulate innovative and trans-European eServices. Priority areas include eGovernment, eHealth, eInclusion, eLearning, Trust and Security and SME‘s.

---

[72] cf. Panayiotou, Panayiotis Andrea, Electronic Governance for the Lands and Surveys Department in Cyprus, FIG Working Week 2004, AThens, Greece, May 22-17, 2004

[73] cf. The European Commission, IDABC, The Programme, http://ec.europa.eu/idabc/en/chapter/3, access on

[74] cf. Commission of the European Communities, Communication form the Commission to the council, the European Parliament, the European economic and social committtee and the commmittee of he regions, i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, 25.04.2006, Brussels

[75] cf. European Commission, Information Society, eTEN Brochure, http://ec.europa.eu/information_society/activities/eten/index_en.htm, access on 1.10.2007, 9:14

1.10.3 Private initiatives

QuEST - Microsoft Qualified Electronic Signature Tutorial initiative

QuEST is a qualified electronic signatures tutorial by Microsoft and helps architects to build solutions integrating electronic signatures.[76]

Microsoft started the Qualified Electronic Signatures Tutorial project to develop solutions that integrate electronic signatures according to the European Directive. [77]

Using a qualified electronic signature that is equivalent to a handwritten one takes a lot of requirements, the purpose of use and policies must be defined. this is rather complex because of different legal, technological and policy issues. QuEST guidelines aims to demystify this area and examines these three perspectives and their correlation with each other.[78]

DIS Belgium

In Belgium, the electronic identity card eID was successfully introduced. Both private and governmental institutions had great interest in applications for authentications and transaction enabled by the eID. But market confidence as well as consumer trust in applications for eGovernment and eBusiness needed to be boosted and therefore, the Digital Identity Standard Institute (DIS) was founded to develop a standard and label that provides customers with assurance. Clear guidelines have been set and afford a better qulaity management of legal, technical and policy aspects of eID applications.[79]

For more information see www.disinstitute.be.

---

[76] cf. Microsoft, QuEST - Qulified Electronic Signatures Tutorial, http://www.microsoft.com/downloads/details.aspx?familyid=0b3c55f6-11d4-4f46-8a37-0ba004e14dcf&displaylang=en, access on 1.10.2007, 9:36

[77] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[78] cf. Microsoft, QuEST - Qualified Electronic Signatures Tutorial, http://www.microsoft.com/downloads/details.aspx?familyid=0b3c55f6-11d4-4f46-8a37-0ba004e14dcf&displaylang=en, access on 1.10.2008, 9:36

[79] cf. ISSEE 2006, Securing Electronic Business Processes, Vierweg 2006

2. Country Analysis: EU members

2.1 Austria

Figure 7: Fact-sheet: Austria, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 7 some basic demographic and geographic data of the country is presented.

2.1.1 Institutional frame

Legislation

Austria was one of the first countries to adopt the directive 1999/93/EG of the European Parliament for the collaborative implementation for electronic signature.
The basic for the recognition of electronic signatures in the Austrian Law is the national law for electronic signatures Signaturgesetz-SigG, BGBl I 1999/190 (see Appendix - Austria: Signaturgesetz SigG)[80]

The Austrian Federal Economic Chamber provides an information film about digital signature and the signature law on http://www.signatur.rtr.at/de/legal/directive.html.

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Austria: Nation Regulations Details.[81]

[80] cf. Study of the Donau Universität Krems, Master-Studie

[81] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•recognition of foreign certificates:[82]
In October 1998, the agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of Online Services

A lot of official channels can be carried out online via the „Bürgerkarte“: application of attestations, registration and signing of persons or vehicles, reception of RSa-letters, filing a tax return (www.help.gv.at).[83]

•eGovernment: The first fully transactional online eGovernment service using the citizen card was the electronic confirmation of residence at https://meldung.cio.gv.at/egovMB.. It uses all basic components (Identification, electronic signature, payment and electronic delivery) of eGovernment, requiring qualified or simple signature on smart card or mobile SIM card.[84]

•FinanzOnline - electronic Tax declarations:[85]
In 2003, a platform for online tax declaration services was launched. In the time period between 2003 and 2006, about 840.000 citizens and 160.000 companies and organizations have been registered for this service. The platform can be accessed at http://finanzonline.bmf.gv.at by simple use of username and password or the Citizen card. If the Citizen Card is used for access a qualified signature is required for log-in.
Altogether, about 1 million users exercise electronic tax declarations using username and Password access and electronic signature.

•www.zustellung.gv.at - electronic delivery service:[86]
The aim is to provide administrative proceedings electronically by a public administration‘s delivery service that was implemented in May 2004.

---

[82] cf. Study of the Donau Universität Krems, Master-Studie, Austria

[83] cf. http://portal.wko.at/wk/sn_detail.wk?AngID=1&DocID=363836&StID=187037, access on 14.11.2007, 16:11

[84] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[85] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[86] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•Statement of pension contribution terms:[87]
On the site http://www.sozialversicherung.at/esvapps/page/page.jsp?p_pageid=110&p_menuid=60845&p_id=5, all periods of contribution to pension accounts can bee queried by using qualified signature on smart card or virtual SIM cards.

•help.gv.at:
The project http://www.help.gv.at is an online administrative assistance, which offers a lot of possibilities to carry out official channels online.[88] Figure 8 shows the main page of the portal.

Figure 8: Welcome page of the portal www.help.gv.at, source: http://www.help.gv.at, access on 4.12.2007 ,18:41

•eProcurement: Also the processing of announcements can be made in accordance with existing law (e.g., www.auftrag.at).[89]

•eShopping: By singing contracts electronically in a web shop less unreliable orders are effected. On the other side, so called server certificates guarantee the identity of a web shop operator.[90]

•eArchiving: Enterprises can store their electronic documents in electronic archiving systems with digital signatures in a secure way.[91]

[87] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[88] cf. http://portal.wko.at/wk/sn_detail.wk?AngID=1&DocID=363836&StID=187037, access on 14.11.2007, 16:11

[89] cf. http://portal.wko.at/wk/sn_detail.wk?AngID=1&DocID=363836&StID=187037, access on 14.11.2007, 16:11

[90] cf. http://portal.wko.at/wk/sn_detail.wk?AngID=1&DocID=363836&StID=187037, access on 14.11.2007, 16:11

[91] cf. http://portal.wko.at/wk/sn_detail.wk?AngID=1&DocID=363836&StID=187037, access on 14.11.2007, 16:11

•online banking: many banks offer the service of digital signature during online banking which is secure and easy, without PINs and TANs.
For example the BAWAG P.S.K. supports the signature card during netbanking.[92]
Nearly all banks (excepting Bank Austria and Erste Bank) are actually offering the insertion of qualified electronic signatures for online banking.[93]

•eHealth:[94]
At the end of 2005, about 8,2 Million eCards have been issued to the austrian population. The eCard is an electronic chip card (figure 9) that replaces the health insurance certificate on paper. Medical services are accessible electronically for insurances and members.

Figure 9: e-card, source: http://www.chipkarte.at/, access on 4.12.2007, 18:49

The e-Card is a electronic health insurance certificate that is used since summer 2005.
A distribution of 8,2 Million e-Cards was planned for 2002 but effected not until 2005.
It is also possible to grade up the card to a citizen card with signature function.

Also the Austrian Chamber of Pharmacists developed a new pharmacist identity card, that is provided with a qualified certificate for the electronic signature and with functionality for the citizen card. This card enables and encourages electronic exchange of health data, an improvement of the access to information about services and planning and report purposes. The pharmacist identity card is designed as „Health-Professional-Card“ that guarantees security when accessing patient data. .It is an international identity card with that pharmacists can identify themselves quickly and unbureaucratly in foreign countries.[95]
In September 2006, the Chamber of Pharmacists started to issue the ID cards and the result is satisfying: With ca. 5.000 active members, about 3.300 orders can be recorded, thereunder 3.000 cards have been activated. But the application of digital signature function is only used marginally.[96]

•eServices:
The Austrian social insurance institution offers a range of electronic services on

[92] cf. http://portal.wko.at/wk/sn_detail.wk?AngID=1&DocID=363836&StID=187037, access on 14.11.2007, 16:11

[93] cf. Correspondance with RTR GmbH, Austrian Regualtory Authority for Broadcasting and Telecommunications, Austria

[94] cf. http://portal.wko.at/wk/sn_detail.wk?AngID=1&DocID=363836&StID=187037, access on 14.11.2007, 16:11

[95] cf. http://www.apotheker.or.at, access on 4.12.2007, 19:13

[96] cf. Correspondence with Dr. Brigitte Wunsch, Abteilung I (Präsidium) der Pharmazeutischen Gehaltskasse für Österreich

http://www.sozialversicherung.at.[97]
All operational and planned eGovernment applications are summed up in the Appendix - Austria: Operational and planned applications.[98]

•a.trust approved:[99]
A.trust has defined a new quality mark (figure 10) for digital signatures that are qualified according to the signature law.

Figure 10: a.trust approved quality mark, source: http://www.a-trust.at/default.asp?lang=GE&ch=3&node=550, access on 06.11.2007, 17:25

The aim of the quality mark is to signify all products that are compliant with the high standards of the Signature law, like the use of a qualified signature on basis of an qualified certificate issued by a accredited certification service provider.

Types of electronic signature

•basic and qualified electronic signature:
The Law for electronic signature distinguishes between the (basic) electronic signature and the secure electronic signature.
The basic electronic signature can serve as verification, but only the secure electronic signature is regarded as equal with signing personally.
The secure electronic signature can not be adopted in every situation. For instance, secure electronic signatures can not be generated automated, as a PIN-entry is necessary to dissolve the signature function. Furthermore, some software components are only available for certain operating systems.
For the basic electronic signature a certificate is normally required that can be integrated in the application for signing.[100]

•advanced electronic signature:
The term advanced electronic signature does not appear in the Austrian Law, but it is defined in the European Law: It is an electronic signature, that bears resemblance to a secure electronic signature, but has not to be generated via chip card and has not to depend on a qualified certificate. The advanced

[97] cf. http://portal.wko.at/wk/sn_detail.wk?AngID=1&DocID=363836&StID=187037, access on 14.11.2007, 16:11

[98] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[99] cf. http://www.a-trust.at/default.asp?lang=GE&ch=3&node=550, access on 06.11.2007, 17:25

[100] cf. Study of the Donau Universität Krems, Master-Studie

electronic signature is mandatory particularly for the electronic transmission of bills. Also for this purpose a certificate of an certification service provider is necessary. Certification Service Providers, that can issue advanced electronic signatures, are denoted with the letter F on the register, controlled by the RTR-GmbH (the supervising authority for electronic signatures in Austria).[101]

•administrative signature (Verwaltungssignatur):
To encourage the use of electronic signature in eGovernment, an administrative signature can be used in administrative procedures. The administrative signature was only a temporary solution until 2008. Also for this signature neither a qualified certificate nor a chip card was mandatory required. To generate an administrative signature, only a „Bürgerkarte“ is necessary that is not necessarily a chip card, but can also exist only virtually (for example the A1 Signature). Administrative signatures can also be created with the e-Card that was issued by the Austrian Social Insurance Institution.[102]

➡Short description: A1 Signature[103]
A1 mobilkom austria enables the use of electronic signature via mobile telephone. This system illustrated the highest mobile application of electronic signature in Austria. Instead of an card reader or a citizen card, the user only requires mobile reception (for signature data) and access to internet (for the online databank).
The certificate is issued according to X.509 v.3, on basis of trusted root certificates by moblikom austria that fulfills all requirements of SigG.
mobilkom austria controls a certificate revocation list, that is actualized daily (on http://www.a1.net/signatur/crl/currentcrl.crl). Also a registry list can be called up to check the status of the A1 SIGNATURE certificate via email to Verzeichnisdienst_A1_SIGNATUR@mobilkom.at.

The service of A1 Signature was phased out on the 27.07.2006 due to a takeover of businesses by Mobilkom AG. The Certification service is continued by the Mobilkom Austria AG.[104]

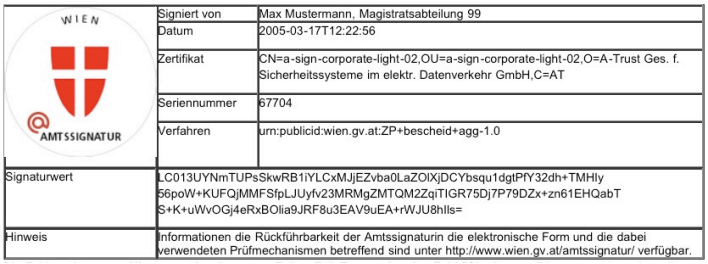
•office signature (Amtssignatur):
Magisterial documents like notifications can be provided with an office signature whose characteristic is the visual presentation.
The office signature can be applied on official notifications and other notices of authorities and denote that it concerns an official document. For example a document that is issued by Vienna City, contains the following office signature (figure 11):

[101] cf. Study of the Donau Universität Krems, Master-Studie

[102] cf. Study of the Donau Universität Krems, Master-Studie

[103] see http://www.a1.net/business/a1signaturablauf, access on 9.11.2007, 15:24

[104] cf. http://www.signatur.rtr.at/de/providers/services/mobilkom-a1signatur.html, access on 9.11.2007, 15:23



	Signiert von	Max Mustermann, Magistratsabteilung 99
	Datum	2005-03-17T12:22:56
	Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Seriennummer	67704
	Verfahren	urn:publicid:wien.gv.at:ZP+bescheid+agg-1.0
Signaturwert	LC013UYNmTUPsSkwRB1iYLCxMJjEZvba0LaZOlXjDCYbsqu1dgtPfY32dh+TMHly 56poW+KUFQjMMFSfpLJUyfv23MRMgZMTQM2ZqiTlGR75Dj7P79DZx+zn61EHQabT S+K+uWvOGj4eRxBOlia9JRF8u3EAV9uEA+rWJU8hIls=	
Hinweis	Informationen die Rückführbarkeit der Amtssignaturin die elektronische Form und die dabei verwendeten Prüfmechanismen betreffend sind unter http://www.wien.gv.at/amtssignatur/ verfügbar.	

Figure 11: Office Signature of Vienna City, source: http://www.wien.gv.at/amtssignatur, access on 09.11.2007, 16:54

•special electronic signatures:[105]

There exist some other electronic signatures only for certain purposes:

- electronic signature of justice (elektronische Signatur der Justiz):It is an advanced electronic signature that is used for juridical transactions.
- electronic authentication signature (elektronische Beurkundungssignatur): It is a secure electronic signature with that solicitors and civil engineers can institute public documents electronically.
- electronic notary signature (elektronische Notarsignatur): This signature is a (specially denoted) secure electronic signature that is used by solicitors for other purposes.
- electronic lawyer signature (elektronische Anwaltssignatur): It is the (specially denoted) secure electronic signature of a lawyer.
- electronic civil engineer signature (elektronische Zivilrechnikersignatur): It is the (specially denoted) secure electronic signature of a civil engineer.

•time stamps:

A time stamp is special form of digital signature, that is created for a special document. For example A-Cert TIMESTAMP operated on basis of the internet standard RFC3161 and collaborates with each RFC3161 compatible software.[106]

If someone decides to acquire a digital signature around 75 € must be brought up. Those cost consist of:[107]

- a.trust signature card: 30€. If one has already a signature compatible Maestro bank card or a Mastercard, those costs drop. If a card is compatible with digital signatures, the card is marked with „a.sign premium“ on its backside (see also Types of secure signature-creation devices).
- Activation costs: one-time 12€.
- Card reader: from 30€ upwards (see Card readers)
- In addition, an annual fee of 15,60 € has to be paid.

[105] cf. Study of the Donau Universität Krems, Master-Studie

[106] cf. http://www.a-cert.at/php/cms_monitor.php?q=FAQ-A-CERT, access on 28.11.2007, 18:38

[107] cf. http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=313671&DstID=0&BrID=513, access on 14.11.2007, 16:11

The Portal FinanzOnline as well as the electronic delivery service zustellung.gv.at use either qualified or simple signature provided by a smart card or a virtual card like a mobile SIM card.
The service of requesting statements of pension contribution terms requires a qualified signature.[108]

2.1.2 Application requirements

Types of certificates

•Qualified Certificates:
To create an electronic signature, a qualified certificate is required to confirm the Identity of the chip card holder.
A qualified certificate assigns the signature creation data clearly to a person. It can only be issued by a Certification Service Provider (Trust Center), that holds an attestation for the issuance of qualified certificates. The qualified certificate is the basic of an secure signature. The Certificates are saved in a publicly accessible data bank (directory service) and is stored on the card of the signatory.
Currently, the A-Trust organization for safety systems for electronic data communication, is the only enterprise that offers qualified certificates with its certification service a.sign Premium (see below - Certification Service Providers). The a.trust is liable for the content of an certificate.
The qualified certificates issued by the a.trust is called trust/sign or a.sign Premium.[109]

Those certificates can be acquired in numerous registration centers, for example branch banks.[110]

•non-qualified certificates:
a.trust also issues non-qualified card- and software certificates. As these certificates also have an high (technological) secure standard and quality in registration, the a.trust denotes those „non-qualified“ certificates as „basic“ certificates.
There are personal certificates (like a.sign token, a.sign light) and certificates that are not issued for a person (automatic basic certificates like server certificates a.sign corporate).[111]

• Key Certificate (Schlüsselzertifikat):
There are two kinds of key certificates: the (qualified) certificate for signature (signature certificate) and the (basic) encryption or secrecy certificate.[112]
Certificates are only valid for a certain period, they can not be renewed. But a new identical certificate can be issued for an existing private key.[113]

---

[108] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[109] cf. Study of the Donau Universität Krems, Master-Studie

[110] cf. Study of the Donau Universität Krems, Master-Studie

[111] cf. Study of the Donau Universität Krems, Master-Studie

[112] cf. Study of the Donau Universität Krems, Master-Studie

[113] cf.: http://www.a-cert.at/php/cms_monitor.php?q=FAQ-A-CERT, access on 28.11.2007, 18:38

Certificates can be obtained at different registration centers, like the Austrian Federal Economic Chamber or certain branch banks. A list of all registration centers can be found at http://www.a-trust.at/registrierung.

The RTR-GmbH generated a graph (figure 12), showing the number of issued certificates, covering the years 2000-2003:[114]

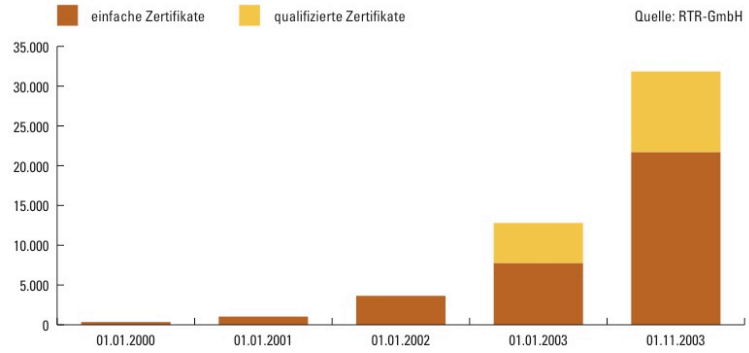


Figure 12: Number of issued certificates in Austria, source: Rundfunk und Telekom Regulierungs GmbH, 4 Jahre Signaturgesetz, Schriftreihe, Band 1/2004

Up to 01.01.2008, about 210.000 valid certificates have been issued by Austrian Certification Service Providers. Thereof, about 66.000 certificates are qualified and 179.000 certificates are stored on secure signature creation devices (chip cards).
According to RTR, most of these certificates are actually used.[115]

Certification Service Providers

The DATAKOM-Austria was the first to provide legal certification in February 2002. Their product was called a-sign and was offered in selected post offices. The fees amount from 7,8€ up to 48€ per year, depending on security grade.
A-Trust, a merger of banks, the Austrian Federal Economic Chamber and others (in total 16 partners), developed a competitor product trust/sign.
But only eighth month afterwards, A-Trust and A-Sign fused and offered their products corporately.
2005, a new certification service provider - A-CERT[116] - entered the market, but the population saw no cause to gain a digital signature. Until mid of 2006, only 65.000 certificates have been issued.
Thereupon, the consulter company DIGISIGN should stimulate demand[117].

[114] cf. Rundfunk und Telekom Regulierungs GmbH, 4 Jahre Signaturgesetz, Schriftreihe, Band 1/2004

[115] cf. Correspondance with RTR GmbH, Austrian Regualtory Authority for Broadcasting and Telecommunications, Austria

[116] see (http://www.a-cert.at)

[117] see http://www.digisign.at

At present, the A-Trust association for safety systems for electronic data transmission GmbH is the only supplier for qualified certificates for secure electronic signatures with its certification service a.sign Premium in Austria.

➡Short description: A-Trust
a.trust is a Trust Center that is conform with the technical and organizational requirements of the Law for electronic signatures. a.trust is an accredited certification authority that has a registration center, a revocation list and a registry service for signature controls. Furthermore, a.trust issues a range of basic certificates apart from qualified digital signature, like server certificates and office signature certificates.
a.trust belongs to austrian banks, industries and chambers.

BEV, the Bundesamt für Eich- und Vermessungswesen, is only issuing secure qualified time stamping services, but the quantity of issued time stamps is not relevant at the moment.[118]

Other Certification Service Provider are listed up in table 4:

Table 4: Certification Service Provider in Austria, source: http://www.signatur.rtr.at/de/providers/providers.html, access on 07.11.2007, 12:37

Certification Service Provider		contact information	Issued certificates
A-Trust		Address: Landstraßer Hauptstraße 5 1030 Wien Telephone: +43 1 713 21 51 0 Fax: +43 1 713 21 51 350 E-Mail: office@a-trust.at Homepage: http://www.a-trust.at/	advanced electronic signature: - a.sign Premium encryption http://www.signatur.rtr.at/de/providers/services/atrust-asign-premium-encryption.html - a.sign token http://www.signatur.rtr.at/de/providers/services/atrust-asign-token.html - a.sign token encryption http://www.signatur.rtr.at/de/providers/services/atrust-asign-token-encryption.html - a.sign corporate light http://www.signatur.rtr.at/de/providers/services/atrust-asign-corporate-light.html) - a.sign corporate medium (for more details see http://www.signatur.rtr.at/de/providers/services/atrust-asign-corporate-medium.html) - a.sign corporate strong http://www.signatur.rtr.at/de/providers/services/atrust-asign-corporate-strong.html

[118] cf. Correspondence with Christine Geyer-Gschladt, Bundesamt für Eich- und Vermessungswesen, Austria

Certification Service Provider		contact information	Issued certificates
			advanced qualified signature: - a.sign Premium http://www.signatur.rtr.at/de/providers/services/atrust-asign-premium.html others: - a.sign SSL http://www.signatur.rtr.at/de/providers/services/atrust-asign-ssl.html - a.sign Company Root http://www.signatur.rtr.at/de/providers/services/atrust-asign-company-root.html - a.sign developer http://www.signatur.rtr.at/de/providers/services/atrust-asign-developer.html - a.sign light http://www.signatur.rtr.at/de/providers/services/atrust-asign-light.html
Bundesamt für Eich- und Vermessungswesen		Address: Schiffamtsgasse 1-3 1025 Wien Telephone: +43 1 21110 0 Fax: +43 1 21110 2199 E-Mail: info@bev.gv.at Homepage: http://www.bev.gv.at/	secure timestamp service
Arge Daten - Österreichische Gesellschaft für Datenschutz (Verein)		Address: Redtenbachergasse 20/27-32 1160 Wien Telephone: +43 676 91 07 032 Fax: +43 1 480 32 09 E-Mail: info@a-cert.at Homepage: http://www.a-cert.at/	advanced electronic signature: - a-cert government (for more details see http://www.signatur.rtr.at/de/providers/services/argedaten-a-cert-government.html) - global trust (for more details see http://www.signatur.rtr.at/de/providers/services/argedaten-globaltrust.html) - a-cert advanced (for more details see http://www.signatur.rtr.at/de/providers/services/argedaten-a-cert-advanced.html) others: - a-cert timestamp (for more details see http://www.signatur.rtr.at/de/providers/services/argedaten-a-cert-timestamp.html) - a-cert (for more details see http://www.signatur.rtr.at/de/providers/services/argedaten-a-cert.html) - a-cert / globaltrust (for more details see http://www.signatur.rtr.at/de/providers/services/argedaten-a-cert-globaltrust.html)

Certification Service Provider		contact information	Issued certificates
Generali IT-Solutions GmbH		Address: PZ-PKI Kratochwjlestraße 4 1220 Wien Telephone: +43 1 534 01 0 Fax: +43 1 534 01 3391 E-Mail: security.support@generali.at Homepage: http://zertifikate.generali.at/	net.surance security (for more details see http://www.signatur.rtr.at/de/providers/services/generali-it-netsurance.html)
Hauptverband der österreichischen Sozialversicherungsträger		Address: Kundmanngasse 21 1031 Wien Telephone: +43 1 711 32 Fax: +43 1 711 32 3777 E-Mail: posteingang.allgemein@hvb.sozvers.at Homepage: http://www.hauptverband.at	advanced electronic signature: - e-Card Verwaltungssignatur (for more details see http://www.signatur.rtr.at/de/providers/services/hauptverband-vsig.html) - e-Card gewöhnliche Signatur (for more details see http://www.signatur.rtr.at/de/providers/services/hauptverband-gsig.html) others: e-Card Vertragspartner Signatur (for more details see http://www.signatur.rtr.at/de/providers/services/hauptverband-vertragspartner.html)
Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie		Address: Technische Universität Graz Inffeldgasse 16 8010 Graz T: +43 316 873 5513 Fax: +43 316 873 5520 E-Mail: europki-info@iaik.at http://europki.iaik.at/	- IAIK EuroPKI TU-Graz Server CA (for more details see http://www.signatur.rtr.at/de/providers/services/iaik-europki-server-ca.html) - IAIK EuroPKI TU-Graz SIG CA (for more details see http://www.signatur.rtr.at/de/providers/services/iaik-europki-sig-ca.html)
Magistrat der Stadt Wien		Address: Rathausstraße 1 1082 Wien Telephone: +43 1 4000 91631 Fax: +43 1 4000 99 91631 E-Mail: pfp@adv.magwien.gv.at Homepage: http://www.wien.gv.at/ma14/zertifikate.html	advanced electronic signature - Benutzer-Signaturen-CA (for more details see http://www.signatur.rtr.at/de/providers/services/wien-benutzer.html) - Externe-CA (for more details see http://www.signatur.rtr.at/de/providers/services/wien-externe.html) others: - Server- und Applikationen-CA (for more details see http://www.signatur.rtr.at/de/providers/services/wien-server.html) also see http://www.wien.gv.at/ma14/zertifikate.html

Certification Service Provider		contact information	Issued certificates
mobilkom austria AG & Co KG		Address: Obere Donaustraße 29 1020 Wien Telephone: +43 1 33161 0 Fax: +43 800 664 681 Homepage: http://www.mobilkomaustria.com/ Status: services of issuing certificates has been shut down	advanced electronic signature: A1-Signature (for more details see http://www.signatur.rtr.at/de/providers/services/mobilkom-a1signatur.html and http://www.a1.net/business/a1signaturmehrdetailszua1signatur)
Trosoft Entwicklungs u. Vertriebs GmbH		Address: Linzer Straße 156 4600 Wels Telephone: +43 7242 239 707 Fax: +43 7229 7229011 E-Mail: info@trosoft.net Homepage: http://www.trosoft.net/ Comment: Change of name in xyzmo Software GmbH on 18.07.2006 Status: nunmehr xyzmo Software GmbH	advanced electronic signatures: - Trodat Seal (for more details see http://www.signatur.rtr.at/de/providers/services/trosoft-trodatseal.html) The certification sercice is now provided under the denotation xyzmo Seal by xyzmo Software GmbH.
XiCrypt Internetsicherheitslösungen GmbH		Address: Hub 109 8046 Graz Telephone: +43 699 24 10 20 20 Fax: +43 316 91 39 76 E-Mail: office@xicrypt.com Homepage: http://www.xicrypt.com/	- XiCrypt Personal CA (for more details see http://www.signatur.rtr.at/de/providers/services/xicrypt-personal.html) - XiCrypt Timestamping Services (for more details see http://www.signatur.rtr.at/de/providers/services/xicrypt-timestamping.html)

Inspecting authorities

The austrian certification service providers are controlled by the Telekom Kontrol Kommission (TKK) in accordance with the Law of signatures (sigG), respectively by RTR GmH.

Furthermore, A-Sit has striven for the accreditation as monitoring institution and received its confirmation on the 25th october 2004. A-Sit supervises the IT-security of electronic payment systems as well as of IT-products and IT-systems.

➡Short description: A-Sit[119]
A-Sit was founded in 1999 as a non-profit society and is operated as a competent center for IT-security. Club members of A-Sit are the

- Federal Ministry of Finance,
- Austrian National Bank,
- Technical University Graz.

Basic principles are

- strict neutrality,
- liberty concerning directives.
- economical autonomy.

2.1.3 Technical preconditions

Signature Software

OpenLimit, the Swiss Holding AG, closed a contract with X.Key GmbH in Vienna to stimulate the diffusion of OpenLimit technologies in Austria. OpenLimits products fulfill essential characteristics: They are certified according to the Common Criteria security standard EAL 4+, support advanced and qualified (secure) electronic signatures in the PDF and PDF/A standard and can be integrated in other applications.[120]

Another supplier of signature software is the enterprise IT Solution GmbH. IT Solution offers different client software like trustDesk, the basic signature package. This package is extendable with plugins like „mulitPFD“ for mass signature for pdf documents or „procure“ for qualified signatures. Other products include Server Software and development modules.[121]

Types of secure signature-creation device

To generate an electronic signature, a chip card (for example a cash card), a card reader and a special software is required.

•„Bürgerkarte“ - a citizen card
The citizen card allows to handle official channels electronically (http://www.help.gv.at).
On http://www.help.gv.at one can find many uses for the citizen card, which include regional and nationwide applications, among others

- issuing of birth certificates,
- request for the change of name,
- request for registration certificates,

---

[119] cf. http://www.a-sit.at/de/allgemein/asit.php, access on 4.12.2007, 18:46

[120] cf. Pressetext, OpenLimit etabliert mit X.Key Vertriebspartnerschaft für Österreich, Press release 21.1.2008, http://www.pressetext.at/pte.mc?pte=080121020, access on 07.11.2007, 14:59

[121] cf. IT solutions, Produkte, http://www.itsolution.at/DE/produkte.html, access on 07.11.2007, 15:18

-request for study aid,
- registration of industries et cetera.[122]

•Health-Professional-Card
This card serves as an identity card for pharmacists and enables identification, secure access to patient data and medical services.

•Lawyer Identity Card
The Lawyer Identity Card is a combination of identity card and electronic signature card. Telekom Austria and the Austrian bar association ÖRAK launched the new card that includes essential functions: It serves as legitimation, as official photo identification and it includes electronic signature with that contracts can be signed legally and transmitted electronically in a secure way. The card is available at the bar associations in all provinces.

•e-Card
The e-Card is a electronic health insurance certificate that is used since summer 2005. Medical services are accessible electronically for insurances and members. It is also possible to grade up the card to a citizen card with signature function, but it was only little demand until October 2006 (only 9.000 certificates).

•StudentID with electronic chip
Student cards, which already displace the student ID on paper on many universities, are equipped like the citizen cards and can be used for signing the erasmus contract.
The Vienna University of Economics and Business Administration issues student cards in chip format since 2000. In line with an e-voting project for the voting for Federal President, the cards were equipped with signature and citizen card functionality. About 20.000 students used this chance.[123]

•OCG member card
In line with a pilot project, the Austrian Computer Society issues member cards (figure 13) with signature and citizen card function since 2002. This card is identical with the citizen card a.sign premium by A-Trust.

Figure 13: OCG member card, source: Gerstbach, Peter, Die österreichische Bürgerkarte, Dezebmer 2004, Wien

•Bank card:
Since the 1th July 2004, all new bank cards are prepared for the functionality of citizen cards.

[122] see http://www.help.gv.at/sigliste

[123] cf. http://e-voting.wu-wien.ac.at/scripts/download.php?F_ID=72, access on 07.11.2007, 19:54

•BusinessCard:[124]

The Business Card (figure 14) is a solution for every kind of Business transaction. PayLife offers different kind of cards: Business MasterCard and Business VISA.

Figure 14: Business MasterCard and Business VISA, source: http://www.kreditkarte.at/plb/export/system/Medien/Dokumente/MasterCard/Folder_und_Antraege/Mulitbrand__WERB_business.pdf, access on 07.11.2007, 18:29

The advantages include world wide payment options: around 31 million points of acceptance, thereof 95.000 in Austria, secure eCommerce with MasterCard SecureCode and verified by VISA, an online portal (mein.kreditkartenportal.at) to see all expenses at a glance and digital signature.

The online Portal for enterprises can be reached at firmen.kreditkartenportal.at. The login on the Portal is effected via token and personal password.

The chip of the card is compatible with electronic signature and the card can be extended with the function of the electronic citizen card. With the citizen card, a lot of services can be used, like eGovernment applications, e-Billing, e-Procurement, e-Contracting and a lot of other e-Services.

Card readers

The regulation authority RTR recommends on its homepage the following card readers that are certified (table 5):

Table 5: Recommended card readers in Austria by RTR, source: http://www.signatur.rtr.at/de/providers/products.html , access on 05.12.2007, 13:03

type of card readers	Producer	mark (models)		connec-tion	supporting operation systems	vendors
PIN Pad	KOBIL	KAAN Profes-sional, Hardware-Version KCT100, Firmware-Version 2.08 GK 1.04		-	Windows 98 to Windows Vista	KOBIL Systems GmbH Weinsheimer Straße 71 D - 67547 Worms Germany Telefon: +49-6241-3004-74 Fax: +49-6241-3004-80 KOBIL Systems GmbH

[124] cf. http://www.kreditkarte.at/plb/export/system/Medien/Dokumente/MasterCard/Folder_und_Antraege/Mulitbrand__WERB_business.pdf, access on 07.11.2007, 18:29

type of card readers	Producer	mark (models)		connec-tion	supporting operation systems	vendors
	Reiner	cyberJack54, Hardware- und Firmware-Version 3.0		-	-	REINER Kartengeräte GmbH und Co. KG Goethestr. 14 D-78120 Furtwangen Telefon: +49 (0)7723 5056-0 Telefax: +49 (0)7723 5056-78 E-Mail: mail@reiner-sct.com Internet: www.reiner-sct.com
PIN Pad, display	Reiner	cyberJack e-com, Hardware- und Firmware-Version 2.0		-	-	REINER Kartengeräte GmbH und Co. KG Goethestr. 14 D-78120 Furtwangen Telefon: +49 (0)7723 5056-0 Telefax: +49 (0)7723 5056-78 E-Mail: mail@reiner-sct.com Internet: www.reiner-sct.com
PIN Pad	Reiner	cyberJack pinpad, Hardware- und Firmware-Version 2.0		-	-	REINER Kartengeräte GmbH und Co. KG Goethestr. 14 D-78120 Furtwangen Telefon: +49 (0)7723 5056-0 Telefax: +49 (0)7723 5056-78 E-Mail: mail@reiner-sct.com Internet: www.reiner-sct.com
	Siemens	Sign@tor Terminal Version 1.0		-	-	-
	Siemens	Sign@tor Terminal Version 2.0		-	-	-

Furthermore, A-Trust recommends additionally the following card readers and advises users to exclusively use card readers with PIN pad for secure signature (table 6).

Table 6: Recommended card readers in Austria by A-Trust, source: http://projekte.a-trust.at/info.asp?lang=GE&ch=2&node=789, access on 05.12.2007, 13:05

type of card readers	Producer	mark (models)		connection	supporting operation sys-tems	detailed information
key-board	Cherry	G83-6700LQZxx/01		PS/2, RS 232	-	http://www.cherry.de/deutsch/produkte/kabeltastaturen_smartboard_g83-6700.htm
		G81-7015LQZxx/01		-	-	-

type of card readers	Producer	mark (models)		connection	supporting operation sys-tems	detailed information
		G81-8015LQZxx/01		seriell	-	-
		G81-12000LTZxx/01		parallel, seriell	-	-
		Smartboard xx44 Familie		-	-	-
	Kobil	KAAN Standard Plus		USB	-	-
		KAAN Advanced		USB	-	-
	Omnikey	CardMan Trust CM3621		USB	Windows 98/ME Windows 2000 Windows XP Windows Server 2003 Windows XP64bit (IA64, AMD64, EM64T) Windows Vista 32bit Windows Vista 64bit Windows CE (hardware-abhängig) Linux	http://omnikey.aaitg.com/index.php?id=products&L=1&tx_okprod_pi1[product]=31
		CM 3821		USB	Windows 98/ME Windows 2000 Windows XP Windows Server 2003 Windows XP64bit (IA64, AMD64, EM64T) Windows Vista 32bit Windows Vista 64bit Windows CE (hardware-abhängig) Linux	http://omnikey.aaitg.com/index.php?id=products&L=1&tx_okprod_pi1[product]=33

type of card readers	Producer	mark (models)		connection	supporting operation systems	detailed information
	SMC Microsystems	Chipdrive SPR532		-	-	-

Certificate requirements

For the Citizen Card a special environment (Bürgerkarten-Umgebung) is required. This Bürgerkarten-Umgebung is a program, that enables access to the citizen card. To effect this, a program has to be installed locally on the users computer.[125]

Application programming interface for online-verification

A1 Signature (phased out):

Mobilkom austria controled a certificate revocation list, that is actualized daily (on http://www.a1.net/signatur/crl/currentcrl.crl). Also a directory service can be called up to check the status of the A1 SIGNATURE certificate via email to Verzeichnisdienst_A1_SIGNATUR@mobilkom.at.

All Certification Service Provider have both a certification revocation list and a directory service on their homepage.

2.1.4 Summary

Table 7 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 7: Summary and rating, Austria, source: own illustration

categories		rating
legal framework	Austria was one of the first country to adopt the EU directive in 1999.	A
technical standard	eGov, eTax, eProcurement, eBanking, eHealth, all types of electronic signatures and certificates, timestamps eCard, different IDcards, 10 CSP, CRL	A

[125] cf. Gerstbach, Peter, Die österreichische Bürgerkarte, Dezebmer 2004, Wien

categories		rating
distribution	The eHealth card can be graded up with signature function, but the application of digital signature function is used marginally. Until mid of 2006, A-Cert issued only 65.000 certificates. The eCard was issued in summer 2005. Until October 2006 only 9.000 certificates have been issued on eCards. Up to 01.01.2008, about 210.000 valid certificates have been issued by all Austrian Certification Service Providers (thereof about 66.000 qualified certificates, 179.000 certificates on SSCD).	B

2.2 Belgium

Figure 15: Fact-sheet: The Belgium, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:49

In figure 15 some basic demographic and geographic data of the country is presented.

2.2.1 Institutional frame

Legislation

The EU directive for electronic signature was implemented in national Law on the 09.07.2001 (see Appendix – Belgium: Law on digital signature), which is a general transposition of the directive. On the 6th December 2002, the law was completed with a Royal Degree for the organization of the control and accreditation of the service providers.[126]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Belgium: National Regulations Details.[127]

Availability of Online Services

•eGovernment:

Belgium established an eGovernment portal that is provided in different languages. It presents actual developments (like the implementation on an electronic passport) and contains all technical standards for the Belgian eGovernment.[128] The main page of the portal can be seen in figure 16.

---

[126] cf. Correspondence with Dirk Leroy, Attaché, FPS Economy, S.M.E.s, Self-employed and Energy Directorate-General Quality and Safety Information Management, Brussels, on 7.11.2007, 15:26

[127] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Belgium, April 2007, source: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[128] cf. http://www.belgium.be/eportal/index.isp, access on 08.08.2007, 15:12

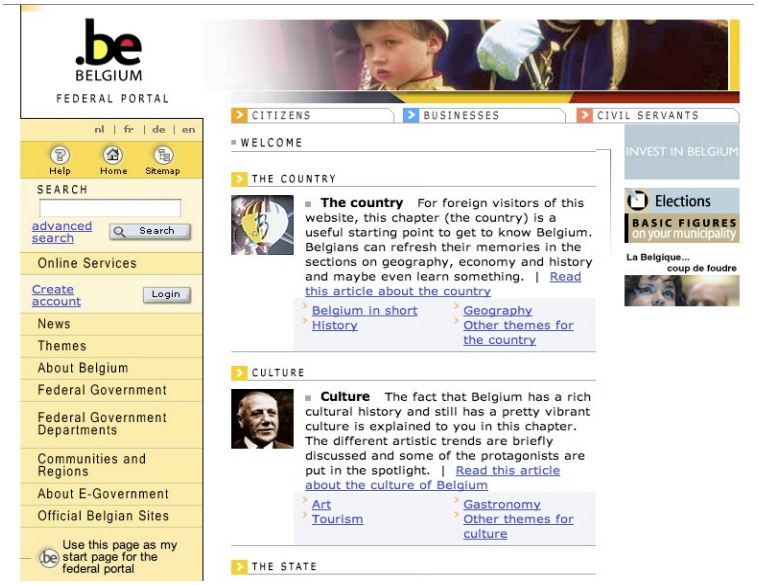


Figure 16: Belgian Federal Portal, source: http://www.belgium.be, access on 05.09.2007, 18:19

•eTax:[129]

On www.taxonweb.be, Belgian residents can declare their personal income taxes online. The service is provided by Federal Public Service Finance and was launched in 2003. Furthermore, taxpayers can calculate their income tax, save data online, submit their tax returns electronically and receive a receipt for the Tax Authority. The Service requires a qualified signature on eID card or a simple signature on on the Federal Token (classifies as advanced electronic signature). In 2005, 569.430 electronic deposits were effected.

•Bornem E-loket[130]

E-loket is a local application in the Commune of Bornem allowing to request official documents like birth certificates or others. To use this service, the user must authenticate through a web interface by using either eID card or the Federal Token. The signed certificates have full legal value and will be handed out as pdf. file. But it has limited practical value as many partners will not accept electronic documents due to a lack of validation mechanism that are easily accessible for such files.

The application was launched in 2004 and since then 422 users have been registered (out of 20.000 citizens. In 2006, 162 requests for civil registers were sent and 122 certificates were distributed for civil affairs.

[129] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Belgium, April 2007, source: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[130] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Belgium, April 2007, source: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•other eServices:
All operational and planned eGovernment applications are summed up in the Appendix- Belgium: Operational and planned applications.[131]

There are also about 400 local or private applications, where electronic signature can be used (community - citizen,employer - employee).[132]

Types of electronic signature

In Belgium exist all types of electronic signature, ranging from basic to secure electronic signature with qualified certificates.[133]
Belgium has one major application for electronic signature, the electronic identity card issued by the Federal Public Service of Interior - the National Register RRN. This card enables the use of qualified signatures. Other applications both governmental as non-governmental use other kind of signatures.[134]
Tax on Web for example require qualified or simple signature on smart cards like the eID card.[135]

2.2.2 Application requirements

Types of certificates

There are hardware certificates, like USB-Token or Smartcards, and accordingly eID (electronic Identity), but also software certificates like the Aladdin software.[136]

Certipost, supplier of digital certificates since 1998, provides a list of available certification types on its webpage (figures 17-22):[137]

---

[131] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[132] cf. Correspondence with Dirk Leroy, Attaché, FPS Economy, S.M.E.s, Self-employed and Energy Directorate-General Quality and Safety Information Management, Brussels

[133] cf. Correspondence with Mag. Peter Fuchs, commercial attaché for Belgium and Luxembourg, Federal Economic Chamber, foreign trade office Brussels

[134] cf. Correspondence with Dirk Leroy, Attaché, FPS Economy, S.M.E.s, Self-employed and Energy Directorate-General Quality and Safety Information Management, Brussels, on 7.11.2007, 15:26

[135] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Belgium, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[136] cf. Correspondence with Mag. Peter Fuchs, commercial attaché for Belgium and Luxembourg, Federal Economic Chamber, foreign trade office Brussels

[137] cf. http://www.e-trust.be/, access on 13.07.2007, 16:07

Which application do you need? / You'll need one of the following products	Submit your declarations to the Government electronically INTERVAT, VENSOC, DIMONA,...	Create signature with legal value equivalent to handwritten signatures Certipost e-Signing service	Create invoices with legal value equivalent to paper invoices Certipost e-Invoicing service	Proof of non-repudiation for e-mails and documents Microsoft Outlook Mozilla	Electronic protection of message communication Bizconnect	Secure your website with SSL webserver certificates Microsoft IIS Apache
1.Qualified on USB Token	✓	✓	✓	✓		
2.Qualified on Smartcard	✓	✓	✓	✓		
3.Qualified on CD-ROM	✓			✓		
4.Lightweight by email					✓	
5.SSL by email						✓

Figure 17: available certification types, Certipost, source: http://www.certipost.be, access on 13.07.07, 16:07

•Qualified certificates on USB Flash Token:

	Product Name+	Price	Buy Now
	**Certipost Qualified Certificate on USB Flash Token 1 GB** • certificate validity: 1 year • memory of the Token: 1 GB • 100 free credits for Certipost services	211,10€	Buy Now!
	**Certipost Qualified Certificate on USB Flash Token 1 GB** • certificate validity: 2 years • memory of the Token: 1 GB • 100 free credits for Certipost services	261,10€	Buy Now!
	**Certipost Qualified Certificate on USB Flash Token 1 GB** • certificate validity: 5 years • memory of the Token: 1 GB • 100 free credits for Certipost services	~~411,10€~~ 369,99€	Buy Now!
	**Certipost Qualified Certificate on USB Token** • certificate validity: 1 year • 100 free credits for Certipost services	151,03€	Buy Now!
	**Certipost Qualified Certificate on USB Token** • certificate validity: 2 years • 100 free credits for Certipost services	201,03€	Buy Now!
	**Certipost Qualified Certificate on USB Token** • certificate validity: 5 years • 100 free credits for Certipost services	~~351,03€~~ 315,93€	Buy Now!

Figure 18: Qualified certificates on USB Flash Token, Certipost, source: http://www.certipost.be, access on 13.07.07, 16:07

•Qualified certificates on Smartcards:

Product Name+	Price	Buy Now
Certipost Qualified Certificate on Smartcard • certificate validity: 1 year • 100 free credits for Certipost services	119,71€	Buy Now!
Certipost Qualified Certificate on Smartcard • certificate validity: 2 years • 100 free credits for Certipost services	169,71€	Buy Now!
Certipost Qualified Certificate on Smartcard • certificate validity: 5 years • 100 free credits for Certipost services	~~319,71€~~ 287,74€	Buy Now!
Certipost Qualified Certificate on Smartcard • with USB Card Reader • certificate validity: 1 year • 100 free credits for Certipost services	145,85€	Buy Now!
Certipost Qualified Certificate on Smartcard • with USB Card Reader • certificate validity: 2 year • 100 free credits for Certipost services	195,85€	Buy Now!
Certipost Qualified Certificate on Smartcard • with USB Card Reader • certificate validity: 5 year • 100 free credits for Certipost services	~~345,85€~~ 311,27€	Buy Now!

Figure 19: Qualified certificates on Smartcards, Certipost, source: http://www.certipost.be, access on 13.07.07, 16:07

•Qualified certificates on CD-ROM:

Product Name+	Price	Buy Now
Certipost Qualified Certificate on CD-ROM • certificate validity: 1 year	99,00€	Buy Now!
Certipost Qualified Certificate on CD-ROM • certificate validity: 2 years	149,00€	Buy Now!
Certipost Qualified Certificate on CD-ROM • certificate validity: 5 years	~~289,00€~~ 269,10€	Buy Now!

Figure 20: Qualified certificates on CD-ROM, Certipost, source: http://www.certipost.be, access on 13.07.07, 16:07

•Lightweight certificate by e-mail:

Figure 21: Lightweight certificate by e-mail, Certipost, source: http://www.certipost.be, access on 13.07.07, 16:07

•SSL certificate by e-mail:

Figure 22: SSL certificate by e-mail, Certipost, source: http://www.certipost.be, access on 13.07.07, 16:07

•Belgian Personal Identity Card Project (BelPIC):

The Belgian Government installs digital certificates on electronic chip cards to hand out as eID cards, KidsID cards or foreigner cards (figure 23). The holder of an electronic chip card can be authenticated and is enabled to create legal electronic signatures.[138] At the end of 2006, over 4 million cards have been issued and about 9 million eID cards to be issued until 2009, this project is one of the largest scheme in Europe.[139]

To sign all the data on the eID cards the RRN eID signing certificate is used. This kind of signature is generated at the creation of the electronic chip card and each time the card is updated. This signature is also necessary to allow official government instances, like municipalities or police, to verify the legitimacy of all data on the eID card.[140]

---

[138] cf. FedCT, EID Hierarchy and Certificate Profiles, February 2006, Ref: EID-DEL-004 - V 3.1

[139] cf. http://www.gemalto.com, access on 25.08.2007, 08:25

[140] cf. FedCT, EID Hierarchy and Certificate Profiles, February 2006, Ref: EID-DEL-004 - V 3.1

Figure 23: Belgian eID card, source: http://www.microsoft.com/belux/fr/eid/what.aspx, access on 09.11.2007, 17:07

By End of 2009, every Belgian citizen will be provided with an electronic ID card with 2 certificates on it, one for authentication and one for electronic signatures. In total, about 8 million qualified certificates will be issued for the eID cards with a validity of 5 years.
In Mars 2008, about 7.8 million eID cards have been issued.
In practice, there is an issuance of 10 million certificates every year to cover stolen, lost or damaged eID cards.[141]

•Public Key Infrastructure:
For issuing certificates, a specific information technology infrastructure was developed, the so-called Public Key Infrastructure (PKI). Furthermore, operational entities, called Certification Authorities (CA) are set up to hand out personalized certificates for the chip cards. The personalized certificate is confirmed by the issuing CA, which is in turn confirmed by the Belgium Root CA of the Belgian Government.[142]

Certification Service Providers

To provide a key and certificate life-cycle management of the eID project, a PKI was implemented.[143]
This kind of certification chain also classifies the Certification Service Providers.
There are three levels of the electronic identity:

1. Belgium Root Certification Authority
   Belgium Root CA
   Certification Service Provider: FEDICT (Federal Overheidsdienst voor ICT)

2. eID operational Certification Authorities
   Citizen CA: Certification Service Provider is Certipost
   Foreign CA: Certification Service Provider is Certipost[144]

3. end entity / user certificates.

---

[141] cf. Correspondence with Dirk Leroy, Attaché, FPS Economy, S.M.E.s, Self-employed and Energy Directorate-General Quality and Safety Information Management, Brussels

[142] cf. FedCT, EID Hierarchy and Certificate Profiles, February 2006, Ref: EID-DEL-004 - V 3.1

[143] cf. FedCT, EID Hierarchy and Certificate Profiles, February 2006, Ref: EID-DEL-004 - V 3.1

[144] cf. Correspondence with Mag. Peter Fuchs, commercial attaché for Belgium and Luxembourg, Federal Economic Chamber, foreign trade office Brussels
also see: http://repository.eid.belgium.be/DE/Index.htm

➡Short description of types of CA:[145]

Citizen CA: issues certificates for citizens older than 12 years (on eID card)
Child CA: issues certificates for citizens younger than 12 years (on the child card)
Foreigner CA: issues certificates to Belgian foreigners older than 12 years (on the resident card)

There are also certificates issued for government and administration purpose.

Government CA: issues certificates to Belgian authorities
Government AA: second government CA that issues certificates ft Belgian authorities for more restricted use (only identity providers, assertion authorities)
Administration CA: issues specific role certificates to grant privileged access to data on the eID cards.

➡Short description: Belgium Root CA:

The Belgium Root CA was designated in 1998 by the Belgian Government as primary Certification Authority. Whenever a Certification Authority issues a personalized certificate, it is assured by the signature of the Belgium Root CA.

The Belgium Root CA is the top authority and issues top level certificates to public authorities, civil servants or citizens, but also to operational CAs that issue end-user certificates.

In the Belgium Root Certification Authority domain, Certipost acts as the Belgium Root CA by order of the Belgian Government.[146]

➡Short description: Certipost

Belgacom and the Belgian Post founded Certipost in 2002 as a Joint Venture. It‘s intent was to develop Internet-services, secure electronic communication, e-government applications and provision of a security over Internet. Belgacom provided the E-Trust Certification Authority and the Post furnished a Postbox platform that is now known as MyCertipost.[147]

The current certification operations include issuance, certification status services and repository.

Table 8 sums all certification service provider in Belgium:

[145] cf. FedCT, Belgium Root CA - Certification Practice Statement, 2003

[146] cf. FedCT, Belgium Root CA - Certification Practice Statement, 2003

[147] cf. Correspondence with Mag. Peter Fuchs, commercial attaché for Belgium and Luxembourg, Federal Economic Chamber, foreign trade office Brussels

Table 8: Certification Service Provider in Belgium, source: Correspondence with Mag. Peter Fuchs, commercial attaché for Belgium and Luxembourg, Federal Economic Chamber, foreign trade office Brussels

Certification Service Provider	Issued certificates
Certipost	Qualified Certificate Profile norm Reference RFC 3039 qualified electronic signature
E-Trust (Certipost)	Certipost e-signing currently only accepts eID signing
Foreigner CA (Certipost)	certificates and Certipost Qualified Certificates

Inspecting authorities

The inspecting authority in Belgium is the *Service public fédéral Economie, PME, Classes moyennes et Energie.*

2.2.3 Technical preconditions

Signature Software

To create electronic signatures also the Aladdin Software can be used.

Types of secure signature-creation device

Public Key Infrastructure (PKI):

To provide a key and certificate life-cycle management of the eID project, a PKI infrastructure was implemented.

The most common devices are USB PKI Token and Smartcards and the eID card.

Card readers

In combination with eID, the electronic identity card, a common card reader without Pin entry is recommended.[148]

But there are several types of card readers available (table 9):[149]

[148] cf. Correspondence with Mag. Peter Fuchs, commercial attaché for Belgium and Luxembourg, Federal Economic Chamber, foreign trade office Brussels

[149] cf. http://www.cardreaders.be/en/default.htm, access on 18.07.2007, 11:12

Table 9: Available card readers in Belgium, source: http://www.cardreaers.be, access on 18.07.2007, 11:12

type of card readers	mark (models)		connection	supporting operation systems	vendors
simple transparent card readers	CardMan® 3021		USB 2.0	Windows® 98 √ Windows® ME √ Windows® 2000√ Windows® XP √ Windows® CE 5.0/ CE.NET(depending on hardware) √ Windows® 64bit(AMD64, EM64T, IA64) √ Linux® √ Mac® OS X √	@rrowUp www.arrowup.be
	Cardman 3121		USB 2.0	Windows 2000, Windows XP, Linux, Mac OS X	@rrowUp www.arrowup.be Roadbyte www.roadbyte.be/?eid=hardware
	Cherry (ST-1044UB)		USB 2.0	Windows 98, Windows Me, Windows 2000, Windows XP, Linux kernel 2.4 en 2.6 met PC/SC Lite 1.1 of 1.2	@rrowUp www.arrowup.be Arena Solutions www.arena-solutions.be Multiprox www.multiprox.be
	ACR30		RS232 USB 1.1	Windows NT4, Windows 98, Windows Me, Windows 2000, Windows XP, Linux kernel 2.4 en 2.6 met PC/SC Lite 1.1 of 1.2	Arena Solutions www.arena-solutions.be Roadbyte www.roadbyte.be/?eid=hardware Zetes www.zetes.be
	ACR38		USB 2.0	Windows NT4, Windows 98, Windows Me, Windows 2000, Windows XP, Linux kernel 2.4 en 2.6 met PC/SC Lite 1.1 of 1.2 & Max OSX 10.1 tot 10.3	Arena Solutions www.arena-solutions.be Zetes www.zetes.be
	Fujitsu-Siemens (SCR USB Solo2 SmartCard)		USB	Windows 2000, Windows XP, Linux (on request)	Fujitsu-Siemens www.fujitsu-siemens.be

type of card readers	mark (models)		connection	supporting operation systems	vendors
	GemPC-Twin		USB 2.0/ RS 232	Windows 95, Windows 98, Windows 98SE, Windows NT4, Windows Me, Windows 2000, Windows XP, Windows CE, Windows Server 2003, Linux Redhat WS 3.0 & 4.0, Linux Suse Professional 9.2, Linux DEBIAN "Sarge" , Mac OS X (10.3 Panther & 10.4 Tiger)	Gemplus www.gemplus.be Netdirect www.netdirect.be/gemplus
	GemPC Serial-SL		RS 232	Windows 95, Windows 98, Windows 98SE, Windows NT4, Windows Me, Windows 2000, Windows XP, Windows Server 2003, Linux Redhat WS 3.0 & 4.0, Linux Suse Professional 9.2, Linux DEBIAN "Sarge"	Gemplus www.gemplus.be Netdirect www.netdirect.be/gemplus
	GemPC USB-SL		USB 2.0	Windows 98, Windows 98SE, Windows Me, Windows 2000, Windows XP, Windows CE, Windows Server 2003, Linux Redhat WS 3.0 & 4.0, Linux Suse Professional 9.2, Linux DEBIAN "Sarge" , Ma-cOS X 10.3 Panther	Gemplus www.gemplus.be Netdirect www.netdirect.be/gemplus
Card readers with `secure pinpad`	Cardman 3821		USB 2.0 Full Speed	Windows 2000, Windows XP, Linux	@rrowUp www.arrowup.be
	SCM (SPR532 Pinpad)		Hybrid USB 2/0 / RS232	Windows 98, Windows Me, Windows 2000, Windows XP, Linux kernel 2.4 en 2.6 met PC/SC Lite 1.1 of 1.2	Arena Solutions www.arena-solutions.be Zetes www.zetes.be
	Certipost (eID Starter Kit Pre-mium)		Enclosure	-	Certipost www.certipost.be
	Certipost (eID Development Kit)		Enclosure	-	Certipost www.certipost.be
	Vasco (DIGIPASS 850)		USB 2.0, with secure pin entry	Windows 98, Windows Me, Windows 2000, Windows XP	Vasco www.vasco.com
	Vasco (FinSAFE)		USB 2.0, with secure pin entry	Windows 98, Windows Me, Windows 2000, Windows XP	Vasco www.vasco.com

type of card readers	mark (models)		connection	supporting operation systems	vendors
	Zetes PASS PCSC (Xiring Xi-Pad)		RS232 , USB 2.0	Windows NT4, Windows 98, Windows Me, Windows 2000 (RS 232) of Windows 98, Windows Me, Windows 2000, Windows XP (USB 2.0)	Arena Solutions www.arena-solutions.be Zetes www.zetes.be
Separate card reades that can be integrated in laptops	Cardman 4040 PCMCIA		PC-Card Type II	Windows 2000, Windows XP, Windows CE (iPAQ), Linux, Mac OS X	@rrowUp www.arrowup.be
	Zetes PASS-PCMCIA (ACR91)		PCMCIA Type II	Windows NT4, Windows 98, Windows Me, Windows 2000, Windows XP,Windows CE	Arena Solutions www.arena-solutions.be Zetes www.zetes.be
	HP		PCMCIA Type II	Windows NT4, Windows 98, Windows Me, Windows 2000, Windows XP, Windows CE	HP www.hp.be
	Fujitsu-Siemens (Ref: S26361-F2432-L700)		-	-	Fujitsu-Siemens www.fujitsu-siemens.be
	GemPC Card		PCMCIA Type II	Windows 98, Windows 98SE, Windows NT4, Windows Me, Windows 2000, Windows XP, Windows Server 2003, Linux Redhat WS 3.0 & 4.0, Linux Suse Professional 9.2, Linux DEBIAN "Sarge"	Gemplus www.gemplus.be Netdirect www.netdirect.be/gemplus IBM www.ibm.com
keyboard integrated card readers	Cherry (G83-6744LUA-BE)		USB 2.0, with secure pin entry	Windows 98, Windows Me, Windows 2000, Windows XP, Linux kernel 2.4 en 2.6 met PC/SC Lite 1.1 of 1.2	@rrowUp www.arrowup.be Arena Solutions www.arena-solutions.be Multiprox www.multiprox.be Zetes www.zetes.be
	HP Compaq (Easy Access SmartCard Key-board)		USB 2.0, with secure pin entry	Windows 98, Windows Me, Windows 2000, Windows XP,	HP www.hp.be
	Fujitsu-Siemens (KBPC CID/CID 2)		USB	Windows 2000, Windows XP	Fujitsu-Siemens www.fujitsu-siemens.be

type of card readers	mark (models)		connection	supporting operation systems	vendors
	Fujitsu-Siemens (KBPC CX)		USB	Windows 2000, Windows XP	Fujitsu-Siemens www.fujitsu-siemens.be
Laptop integrated card readers	HP Compaq (business note-book nc6220)		HP Note-book with integrated Card reader	Windows 2000, Windows XP	HP www.hp.be
	HP Compaq (business note-book nc8230)		HP Note-book with integrated Card reader	Windows 2000, Windows XP	HP www.hp.be
	HP Compaq (business note-book nx8220)		HP Note-book with integrated Card reader	Windows 2000, Windows XP	HP www.hp.be
heavy duty kiosk and vending integrated card readers	Heavy Duty e-ID		USB 2.0/ RS 232	Windows NT4, Windows 98, Windows Me, Windows 2000, Windows XP, Linux , Max OSX 10.1 to 10.4	EUTRONIX www.eutronix.be

Certificate requirements

In order to use the eID and the card readers, specific software must be installed, which is free for download from the internet on http://www.cardreaders.be/en/default.htm.

The eID card uses JavaCard technology for Microsoft applications (Internet Explorer, Outlook, ...) and a standard interface for Netscape, Modzilla, Linux, Sun and other open source applications.[150]

Application programming interface for online-verification

To check a certification status online you can use the Certificate Status Web Service on http://status.eid.belgium.be/cert/index.php?lang=en.[151]

On the web-page http://status.eid.belgium.be/crl/index.php a certificate revocation list lookup service. By providing some information (date, time) and entering the certificate serial number you can verify the certificate.[152]

[150] cf. Correspondence with Dirk Leroy, Attaché, FPS Economy, S.M.E.s, Self-employed and Energy Directorate-General Quality and Safety Information Management, Brussels, on 7.11.2007, 15:26

[151] cf. http://status.eid.belgium.be/cert/index.php?lang=en, access on 08.08.07, 13:26

[152] cf. http://status.eid.belgium.be/crl/index.php , access on 08.08.07, 13:26

These two services are summed up on the web page by Certipost for eID services, where you can also find general information about digital certificates, you can download certificates or by test cards. [153]

2.2.4 Summary

Table 10 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 10: Summary and rating, Belgium, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2001.	A
technical standard	eGov, eTax, eServices, over 400 local or private applications all types of electronic signature, Hard- and software certificates eID card, USB Token, other smartcards CRL, OCSP	A
distribution	The Belgian Personal Identity Card has been issued to over 4 million citizens until 2004. It is the largest scheme in Euorpe. In 2005, 569.430 electronic deposits for electronic tax declarations were effected, using either qualified (eID Card) or advanced electronic signatures (Federal Token). In Mars 2008, about 7.8 million eID cards have been issued. In practictice, 10 million certificates are issued every year.	A

[153] cf. http://repository.eid.belgium.be , access on 08.08.07, 13:24

2.3 Bulgaria

Figure 24: Fact-sheet: Bulgaria, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:49

In figure 24 some basic demographic and geographic data of the country is presented.

2.3.1 Institutional frame

Legislation

The Bulgarian Act for electronic document and e-signature (see Appendix – Bulgaria: Law on Electronic Document and Electronic Signature)was passed on 8th of October 2001. It allows to place new services and to optimize operations in the administration.

By virtue of the Bulgarian law e-documents can be signed differently: with common, improved or universal electronic signature.
The common e-signature is coordinated only between the author and the receiver of the electronic document.
The improved e-signature is based on certificates, issued by a Certification Authority.
The universal e-signature is based on certificates that are issued by a CA and registered in the State Commission of Telecommunication.[154]

Referring to the e-government services, characterized above, the universal electronic signature must be specified. The universal electronic signature, as it is defined in the Act for electronic document and e-signature is usable only for the administrative services that are provided by the Bulgarian government. In

[154] cf. National Association of Local Authorities in Denmark et al, Nikolova, Maria, The E-Era and Bulgarian administration, Public Management Forum, A Review for Public Administration Practitioners in Centras and Eastern Europe and the CIS, Vol. VII, No. 2-3 December 2002

2006, the Ministry of State administration and Administrative Reform issues more then 2000 electronic signatures.

But the court does not recognize universal electronic signature as legal signing for contracts. Therefore, universal electronic signature has no use in the B2B or B2C segment. Also trade legislation does only recognize contracts on paper or oral agreements, but no contracts that are electronically signed.[155]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Bulgaria: National Regulations Details.[156]

Availability of online services

•e-Government:

In 2003, the Bulgarian government adopted an e-Government strategy. By the end of 2005, following EU policies, 20 administrative services were elaborated as e-Government services, 8 of them for businesses and 12 services for citizens. In 2005, the 8 on-line services of the e-Government were provided for 80.6% (see table below). 2006, already 25,000 companies submitted their electronically signed value added tax (VAT) documentation via Internet (which means 25% of all Bulgarian companies that are registered for VAT).[157] This development is shown in table 11:

Table 11: e-Government Services, source: CCICMT, e-Government Report, December 2005

Service Category	2003	2004	2005
to citizens (12 type of services)	43.9%	58.0%	47.06%
to businesses (8-types of services)	34.0%	43.0%	80.56%
total (20 types of services)	39,4%	51.0%	58.65%

The eGovernmental portal is accessible at http://egateway.government.bg providing access to different eGovernment services. Some of them require the use of electronic signature like

- change of address
- submissions to the Ministry of Transport
- submissions to the Ministry of state policy.

•public procurement:[158]

On http://smallsrv.minfin.bg an electronic market for small procurements can be found providing information about the requirements and status of published public procurements. Users have the

[155] cf. Spassov, Kamen Boyanov, Seaul, Application of the Digital Opportunity Index to Bulgaria, Sept 1, 2006

[156] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[157] cf. Spassov, Kamen Boyanov, Seaul, Application of the Digital Opportunity Index to Bulgaria, Sept 1, 2006

[158] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Bulgaria, April 2007: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

possibility to submit offers for responding to a specific public procurement, signing it with an universal electronic signature based on a qualified certificate.[159]

•eTax:[160]
Trough the eGovernment application https://inetdec.taxadmin.minfin.bg every citizen can submit personal or corporate income tax declarations. To fill out those electronic declarations, qualified certificates are required to confirm each step during the procedure. The financial documents that are attached to the file must be signed with electronic signature. also the declaration must be signed before being submitted.
Also VAT declarations and diaries can be submitted on this platform.

•Social Security Declaration:[161]
Declarations concerning social security payments can be submitted via http://www.nssi.bg by filling in electronic forms using qualified certificates.

•ePortal of Employment Agency:[162]
This ePortal is available at www.nsz.government.bg/micsy through the webpage of the Employment Agency. Via this platform, requests, proposals and complaints can be submitted requiring registration or the use of an universal electronic signature based on qualified certificates.

Types of electronic signature

The Act for electronic documents and e-signatures implies the three types of electronic signature: common, improved and universal e-signature.

To be able to use e-Government services, people and businesses must have electronic signature. 2006, 21% of the Bulgarian companies had already electronic signature (figure 25). At first people expressed their criticism, but because of all benefits, that electronic signature implies, only 10% of users remain sceptic.[163]

[159] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Bulgaria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[160] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Bulgaria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[161] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Bulgaria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[162] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Bulgaria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[163] cf. Spassov, Kamen Boyanov, Seaul, Application of the Digital Opportunity Index to Bulgaria, Sept 1, 2006

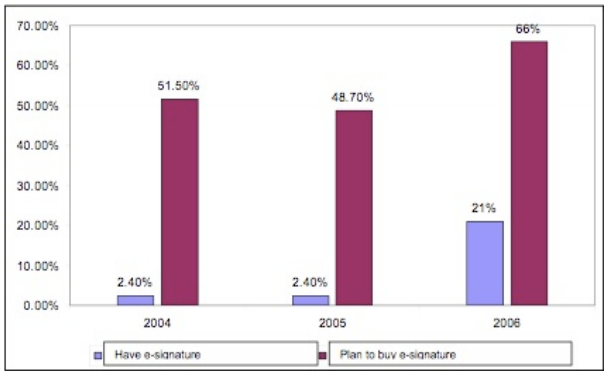


Figure:25: Business and electronic signature usage, source: Estate, January, 2004, February-March, 2005 and Alfa Research, January, 2006

The potential strength of e-signature gives the possibility for building a Public Key Infrastructure in Bulgaria.
But actual there are some obstacles concerning the diffusion of electronic signature, both technically, culturally and organizational.
Up to the present, the Bulgarian authority was not in need of organizational structure, that support e-documents. A general standard for certification is not given and the data exchange between different systems not possible. Currently, some projects are in operation to improve relationship between administration authorities and citizens and make electronic signature common.[164]

2.3.2 Application requirements

Types of certificates

The Bulgarian Academic Certification Authority issues user-, host- and service certificates. SSL-certificates are offered.[165]

The eGovernment application for electronic submission of income tax declarations, the application for small public procurements, the VAT declaration service, the Social security declaration system and many services more requires qualified certificates.[166]

The term „software certificate“ is not common.[167]

---

[164] cf. National Association of Local Authorities in Denmark et al, Nikolova, Maria, The E-Era and Bulgarian administration, Public Management Forum, A Review for Public Administration Practitioners in Centras and Eastern Europe and the CIS, Vol. VII, No. 2-3 December 2002

[165] cf. Correspondence with Vladimir G. Dimitrov, Bulgarian Academy of Sciences, Sofia, Bulgaria

[166] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Bulgaria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[167] cf. Correspondence with Vladimir G. Dimitrov, Bulgarian Academy of Sciences, Sofia, Bulgaria

Certification Service Providers

➡Short description: Bulgarian Academic Certification Authority (BG.ACAD CA)[168]

It is located in the Institute for parallel processing, Bulgarian Academy of Sciences, Sofia, Bulgaria.

The BG.ACAD CA is a research and educational institution, with main activities in Parallel Algorithms, High Performance Computer Architectures, Scientific Computations, Distributed Computing System and Networks, Grid Computing, Linguistic Modeling, Mathematical Methods for Sensor Information Processing.

Furthermore, the BG.ACAD CA is operation a root Certification Authority for Bulgaria, concerned mainly in the area of Grid Computing and research activities. It issues, manages and revocates user-, host-, and service certificates.

The first two official Certificate Authorities in Bulgaria were the Information Service PLC and the Bank-service PLC.

➡Short description: Information Services PLC[169]

It is an official Certificate Authority and exists since 2003, The services by this CA range from issuing certificates for digital signatures, development of related software, selling of appropriated smart-card readers etc. The certificates issued by the Information Services PLC are also used for governmental purpose, for example the ePay and Tax-pay services, offered by the Financial Government of Bulgaria.

➡Short description: Bankservices PLC[170]

Bankservices PLC, is an Automated Clearing House of Bulgarian Banks, a corporation of some national banks. It was registered by the Commission for Regulation of Communication under the Act for Electronic Document and Electronic Signature as a Certification Provider.

The Bulgarian Certificate Authority issues certificates of the enterprise Global Sign, a worldwide Certification Authority. But there are only a few clients as a result of little diffusion and use of electronic signature.[171]

➡Short description: Trust-centre Info-Notary[172]

InfoNotary is a Certificate Service Provider and the biggest private trust-centre in Bulgaria. One of its clients is the governmental administrative authority.

Their services include complete solutions, including PKI architecture, IT security, Secure e-mail, Document signing, Certification and Data encryption and some other services.

InfoNotary PLC is a leading IT security company with more than 400 offices.

---

[168] cf. Correspondence with Vladimir G. Dimitrov, Bulgarian Academy of Sciences, Sofia, Bulgaria

[169] cf. http://stampit.org, access on 18.07.07, 19:20

[170] cf http://www.b-trust.org, access on 18.07.07, 19:34

[171] cf. National Association of Local Authorities in Denmark et al, Nikolova, Maria, The E-Era and Bulgarian administration, Public Management Forum, A Review for Public Administration Practitioners in Centras and Eastern Europe and the CIS, Vol. VII, No. 2-3 December 2002

[172] cf. http://www.infonotary.com, access on 19.07.07, 11:12

The following table (table 12) lists up all certification service providers in Bulgaria.

Table 12: Certification Service Provider in Bulgaria, source: own illustration

Certification Service Providers		Issued certificates
Bulgarian Academic Certification Authority		user-, host-, service certificates SSL certificates
Information Services PLC www.stamplT.org		n.a.
Bankservices PLC www.btrust.org		n.a.
InfoNotary www.infonotary.com		n.a.
Spektar www.spektar.org		n.a.

Inspecting authorities

The Communications Regulation Commission undertakes regulation and control of Certification Service Provider.

2.3.3 Technical preconditions

Signature Software

The Bulgarian Academic Certification Authority offers software, a standard Open SSL package.[173]

InfoNotary offers e-Doc Signer, a software for signing and checking electronic documents. e-Doc Signer is operating on MS Windows and permits signing of any file. For more information see http://www.infonotary.com/site/en/?p=doc_12_4.

Types of secure signature-creation device

In Bulgaria the eGovernment applications like eTax system or eProcurement use smartcards.[174]

•HiPath Security Smartcards:

The both trust centers B-Trust and InfoNotary have certificated the HiPath Security Smart Cards by Siemens. They sell these HiPath Security Smartcards as a part of the Public Key Infrastructure and signature solution.

[173] cf. Correspondence with Vladimir G. Dimitrov, Bulgarian Academy of Sciences, Sofia, Bulgaria

[174] cf. European Commission, IDABC, Token Type, http://ec.europa.eu/idabc/en/chapter/6004, access on 23.11.2007, 13:32

B-Trust and InfoNotary use the both operating systems HiPath Security Card OS as well as Card API. Card OS supports the authentication in networks, the encryption and the digital signature of sensible data and e-mails. Card API improves the use of public-key-technology in combination with CardOS. It provides all necessary interfaces for realizing encryption, authentication and digital signature in conjunction with common business applications. The technique of the 2048-Bit-Encrypting-algorithm of CardOS was critical for the certification.[175]

The Network Consulting Group (NCGroup) sells the products of its partner E-Lock and ActivIdentity, One of its products is the ActiveCard (see table 13, for more information visit: http://www.ncgbg.com/html/activcard.html).[176]

Table 13: ActiveCard specifications, source: http://www.ncgbg.com/html/activcard.html, access on 25.08.2007,08:17

Provider	SSCD		Operating System
NCGroup, ActivIdentity	ActivCard		Windows, Linux, Mac, Solaris

Card readers

In Bulgaria, card readers with a secure PIN-entry are available, but they are not mandatory.[177]

To read the Active Card, the following card readers are recommended, listed up in table 14:

Table 14: recommended card readers for ActiveCard, NCGroup, access on 25.08.2007,08:17

Provider	Model		Connection	Supported OS
ActivIdentity	ActivIdentity USB Reader		USB	Windows 95 Windows Me Windows NT 4 Windows 2000 Windows XP Solaris
	ActivIdentity PCMCIA Reader		PCMCIA	Windows 95 Windows 98 Windows Me Windows NT 4 Windows 2000 Windows XP
	ActivReader™ with ActivIdentity Gold/Token Application			
	ActivReader™ solo			

[175] cf. http://www.omnicard.de/index.php?m=88&id=1612&suchwort=, access on 18.07.2007, 15:32

[176] cf. Correspondence with George Obretinchev, Network Consulting Group, Bulgaria

[177] cf. Correspondence with George Obretinchev, Network Consulting Group, Bulgaria

Certificate requirements

n.a.

Application programming interface for online-verification

The Bulgarian Academic Certificate Authority shows up to date a plain revocation list. Online Tools or an application-programming interface for an online verification is currently not provided.[178]

Also the Information Service PLC offers a CRL.

2.3.4 Summary

Table 15 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 15: Summary and rating, Bulgaria, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2001 by the Bulgarian Act for Electronic Document and eSignature. Court does not recognize ES as legal signing -> no use in B2B, B2C.	C
technical standard	Currently no need of structure that supports e-documents, no general standard for certification, electronic data exchange between different systems not possible, eGov, eTax, eServices, electronic public procurement common, improved and universal signature (based on qualified signatures) range of CSP Smartcards do exist as a part of the PKI and some smartcard readers are recommended. CRL, but online verification currently not provided	B
distribution	eGovernment strategy, by end of 2005: 20 administrative online services, 25% of Bulgarian companies submitted VAT documentation electronically. 2006, 21% of companies had electronic signature In 2006, more than 2.000 eS have been issued by the Ministry of State Administration and Administrative Reform for administrative services. But some obstacles concerning the diffusion of eS, both technically, culturally and organisational. Currently no need of structure that supports e-documents, no general standard for certification, electronic data exchange between different systems not possible, few clients of CSP as result of little diffusion and use of eS	B

[178] cf. Correspondence with Vladimir G. Dimitrov, Bulgarian Academy of Sciences, Sofia, Bulgaria

2.4 Cyprus

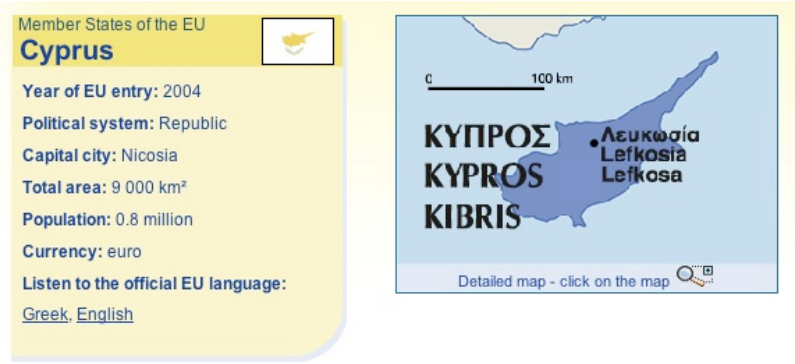


Figure 26: Fact-sheet: Cyprus, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 26 some basic demographic and geographic data of the country is presented.

2.4.1 Institutional frame

Legislation

Cyprus implemented the EU Directive into domestic law in 2004 by the „Law 188 (1)/2004 on the Legal Framework of E-Signature and relevant issues".[179]

An advanced electronic signature that is based on a qualified certificate and created by a secure signature creation device has same legal value as a handwritten signature[180]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Cyprus: National Regulations Details.[181]

Availability of Online Services

•eGovernment: [182]

In 1987, The Government of Cyprus prepared an eGovernment Strategic Plan that was updated in 2002

[179] cf. Neocleous, Andreas, & Co, Cyprus: E-Signature, 08.Nov.2006, Article on http://www.mondaq.com/article.asp?article_id=44032, access on 06.11.2007, 19:58

[180] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Cyprus, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[181] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[182] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Cyprus, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

and in 2004. The main focus was on the examination of information needs of the Government and on the identification of candidate applications. The Government wants to deliver non-stop services to the wide public via Internet and electronic channels like call centers or citizen support centers.
Recently, a National Strategy for Information Society has been developed to develop a framework for electronic transactions and communications services between citizens, businesses and the state and to introduce a computerizes system in Public Administration.

Currently, no eGovernment service in Cyprus uses electronic signature.[183]

All operational and planned eGovernment applications are summed up in the Appendix - Cyprus: Operational and planned applications.[184]

Types of electronic signature

The law recognizes the following three types of electronic signature:
1. electronic signature
2. advanced electronic signature, based on a qualified certificate, created by a secure signature creation device
3. qualified electronic signature.[185]

2.4.2 Application requirements

Types of certificates

And advanced electronic signature is based on a qualified certificate and created by a secure signature creation device. To be qualified, the certificate must be issued by a certification service provider.[186]

Certification Service Providers

n.a.

Table 16 lists up all certification service providers in Cyprus.

Table 16: Certification Service Provider in Cyprus, source: own illustration

Country	Certification Service Provider	Issued Certificates
Cyprus	n.a.	n.a.

[183] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Cyprus, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[184] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[185] cf. Andreas Neocleous & Co, Cyprus: E-Signature, Mondaq, 08.11.2006, http://www.mondaq.com/article.asp?articleid=44032, access on 06.11.2007, 19:58

[186] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Cyprus, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Inspecting authorities

The Ministry of Commerce Industry and Tourism (MCIT) supervises and monitors the certification service providers and examines the adherence of electronic signature with technological and legal requirements defined in the law.[187]

2.4.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

n.a.

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

2.4.4 Summary

Table 17 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 17: Summary and rating, Cyprus, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2004.	A
technical standard	eGovernment Strategic Plan currently no eGov services using eS	C
distribution	-	-

[187] cf. Neocleous, Andreas, & Co, Cyprus: E-Signature, 08.Nov.2006, Article on http://www.mondaq.com/article.asp?article_id=44032, access on 06.11.2007, 19:58

2.5 The Czech Republic

Figure 27: Fact-sheet: The Czech Republic, source: http://europa.eu/abc/european_countries/index_en.htm,, access on 21.08.07, 08:49

In figure 27 some basic demographic and geographic data of the country is presented.

2.5.1 Institutional frame

Legislation

The Czech Parliament adopted the Law on Electronic Signatures on the Basis of EU Directive in May 2000. On September 2001, the Electronic Signatures Act (see Appendix – The Czech Republic: Electronic Signatures Act) came into force.

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - The Czech Republic: National Regulations Details.[188]

•recognition of foreign certificates:[189]

In October 1998, the agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,

[188] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[189] cf. Study of the Donau Universität Krems, Master-Studie, Austria

- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of Online Services

•DIS - Government Gateway:[190]

Clients can submit their deliveries to the Czech Social Security Administration CSSZ via http://www.cssz.cz/epodani/epodani.asp using advanced electronic signature based on qualified software certificates or qualified certificates on smart cards.

Currently, about 40.000 users are registered to the the Gateway, but not everyone uses the system actually.

•public procurement:[191]

www.isvzus.cz is an online information system on public procurement publishing standard forms. The service requires a qualified certificate, either software or hardware certificate. If the contraction authority uses electronic means and tools to send the standard form to the provider, an advanced electronic signature that is based on a qualified certificate is necessary.

In 2005, 28% of forms were sent electronically, provided with an advanced electronic Signature based on a qualified certificate. In the first half of 2006, already 42%, in the second half of the year 2006, more than 50% of the standard forms were send electronically using advanced electronic signature.

•eTax:[192]

All kind of taxes can be electronically declared via http://adis.mfcr.cz/adis/jepo This service is provided by Czech Tax Administration and was launched in 2003 (first only for selected taxes, afterwards the system was extended). The service requires an electronic signature based on a qualified certificate that could be saved electronically (software certificate).

The overall number of electronically submitted tax declarations that contain an electronic signature is 138.558 forms.

Types of electronic signature

The Czech Republic wants to provide citizens with a safe eGovernment service and introduced a service for e-signature and e-stamp authentication. The most important agency for the implementation of electronic signature is the Czech Ministry of the Interior. It wants to provide all public authorities with this service. With an effective authentication system, government authorities can accept electronic

[190] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile The Czech Republic, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[191] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile The Czech Republic, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[192] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile The Czech Republic, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

submissions, deliver documents to e-addresses, issue administrative actions electronically and so on. Currently, the system is mainly used for fiscal administration.[193]

The Czech Republic's Public Administration Portal (http://portal.gov.cz) is including links to a range of services of public institutions that provide electronic communication between public administration bodies and entrepreneurs. Via the portal it is possible to submit tax returns and customs declarations electronically. The number of electronically sent tax returns is growing every day.[194]
The government gateway DIS requires advanced electronic signature that is based on qualified certificates or on commercial certificates of the Czech Social Security Administration.[195]
About 74% of transmitted documents are already signed with an advances electronic signature.[196]

The Greek Certification Service Provider ADACOM S.A. was approved by the Czech Arbitration Court, in order to provide electronic signatures to European users that seek to resolve disputes regarding .eu domain names. ADACOM S.A was listed as the first and, at present, the only Certification Service Provider in Europe, with products that have been successfully tested for compliance with on-line platform of the Czech Arbitration Court. For more information see http://www.adr.eu/adr/electronic_signatures/index.php.[197]

2.5.2 Application requirements

Types of certificates

In the Czech Republic, the different Certification Service provider issue:

- qualified certificates
- qualified system certificates
- qualified time stamps

Results of verification of valid qualified system certificates of accredited providers of certification services are published on http://www.micr.cz/scripts/detail.php?id=3530.[198]

The government gateway DIS requires advanced electronic signature that is based on qualified certificates or on commercial certificates issued by the Czech Social Security Administration. The

[193] cf. Höpner, Petra, Study PKI and Certificate Usage in Europe 2006, Fraunhofer Institute FOKUS, 2006

[194] cf. http://www.mfcr.cz/cps/rde/xchg/mfcr/hs.xsl/conv_program_13457.html, access on 25.08.08, 23:43

[195] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Czech, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[196] cf. http://www.mfcr.cz/cps/rde/xchg/mfcr/hs.xsl/conv_program_13457.html, access on 25.08.08, 23:43

[197] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece,

[198] cf. Correspondence with Mag. Rosmarie Netzer, commercial attaché for the Czech Republic, Federal Economic Chamber, foreign trade office in Prague

certificates can either be software certificates or stored on smart cards. The qualified certificate is valid for 1 year, certificates issued by the Czech Social Security Administration is valid for 3 years.[199]

The electronic Public procurement system requires an advanced electronic signature based on qualified certificates if the contracting authority uses electronic tools for sending standard forms to the provider. The eTax system requires electronic signature based on a qualified software certificate.[200]

The Certification Policies of the Certification Service Provider eIdentity can be found at http://www.eidentity.cz:443/external.svc?page=Cpolitic&sp=SQCA.

The Certification policies of PostSignum can be found at http://qca.postsignum.cz/www/certpolicies.php.

Certification Service Providers

The Ministry of Informatics publishes a review of accreditation granted by the law pursuant to Section 9 (2) letter (e) of the Act No. 227/2000 Coll.[201]

The three accredited certification authorities are: První certifikační autorita, a. s., Česká pošta (PostSignum Qualified CertificatesA), s. p. and eIdentity a. s. (table 18):

Table 18: Certification Service Provider in the Czech Republic, source: http://www.micr.cz/scripts/detail.php?id=3525, access on 15.08.2007, 14:17

Certification Authority		Certificate
První certifikační autorita, a. s., Identification Number 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Prague 9	CERTIFICATION I·CA AUTHORITY	qualified certificates qualified system certificates qualified time stamps
Česká pošta, s. p. Identification Number 47 11 49 83, Olšanská 38/9, PSČ 225 99 Prague 3	POST SIGNUM	qualified certificates. qualified system certificates
eIdentity a. s., Identification Number 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Prague 3	eIdentity	qualified certificates qualified system certificates

[199] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Czech, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[200] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile The Czech Republic, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[201] cf. http://www.micr.cz/scripts/detail.php?id=3525, access on 15.08.07, 14:17

Inspecting authorities

Body for voluntary accreditation, supervision and determination of conformity of SSCDs is the Ministry of Informatics.

2.5.3 Technical preconditions

Signature software

n.a.

Types of secure signature-creation device

Currently, the Czech Ministry of Labour and Social Affairs is the only state organization that uses chip card in a great number. The main use for the ministerial eID cards is to grant access to the ministry's information system or to exchange information within the ministry.[202]

eGovernment applications in the Czech Republic use smartcard, like the DIS system, but also software certificates are in use.

Card readers

Monet+ Smart Card Technology, Gemaltos master retailer for the Czech Republic for smart card readers, recommends the following products (table 19):

Table 19: recommended smart card readers, Monet+, source: http://www.monetplus.com//hw_ctecky_gem.htm, access on 25.08.2007, 23:49

Provider	Model		connection	technical details
Monet+, Gemalto	GemPC Card (PCMCIA)		PCMCIA	PC card reader smart card reader ISO 7816-1,2,3,4 T=0,1 protocols, EMV, synchronous communication rate 9 600 - 115 200 Baudů memory uo to 128 kB (version F) PCMCIA type II interface PC/SC API protocol support certified for Microsoft OS

[202] cf. Höpner, Petra, Study PKI and Certificate Usage in Europe 2006, Fraunhofer Institute FOKUS, 2006

Provider	Model		connection	technical details
	GemPC Twin		USB, RS	Plug&Play reader with USB or RS232 connection connection depends on selecting the cable PC/SC API protocol support communication rate 9,600 – 115,200 bauds power supply through USB or PS/2 port guarantee of 100,000 insertion cycles reads from and writes to all ISO 7816-1,2,3,4, T=0 and T=1, EMV 3.11 ISO 7816 class A,B, and C MS Windows certification
	GemPC Serial - SL		RS	Plug&Play compact smart card reader with RS232 connection communication rate 9,600 – 115,200 bauds power supply through PS/2 port guarantee of 100,000 insertion cycles reads from and writes to all ISO 7816-1,2,3,4, T=0 a T=1, EMV 3.11 ISO 7816 class A,B, and C PC/SC API protocol support MS Windows certification
	GemPC USB - SL		USB	Plug&Play compact smart card reader with USB connection communication rate 9,600 – 115,200 bauds power supply through USB port guarantee of 100,000 insertion cycles reads from and writes to all ISO 7816-1,2,3,4, T=0 a T=1, EMV 3.11 ISO 7816 class A,B, and C PC/SC API protocol support MS Windows certification
	GemPC Key		USB	New, portable PC/SC smart card reader that is connected directly into the USB port and is suitable for "PC Logon" applications. use of smart cards in Plug-in format ISO 7816 class A,B, and C ISO 7816 TA1 support (up to 344 Kbds) reads from and writes to all ISO 7816-1,2,3,4, T=0 a T=1 support of USB full speed USB type A connector, guarantee of 1,500 connection cycles, power supply through USB port certified for Windows OS PC/SC API interface support

Provider	Model		connection	technical details
	GemSelf700 MS-2		RS	Multi-applicational smart card reader with 2 integrated readers, display and keypad. provided with 2 slots for SAM (MS-2) or with 4 slots for SAM (MS-4); two RS232 serial ports with programmable baud rate (9,600 – 38,400) guarantee of 100,000 insertion cycles reads from and writes to all ISO 7816-1,2,3,4 both synchronous and asynchronous (T=0 and T=1) communication rate 9,600 – 115,200 bauds (GemCore technology) LCD display, 2x16 characters keypad with 10 num. and 6 programs. keys buzzer external power supply 9V Attention: no PC/SC API support
Monet +, Omnikey	Omnikey Cardman 4040		PCMCIA	Plug&Play smart card reader of PCMCIA II type with PC/SC interface support and certification for Windows, designed for portable PCs (laptops).
	Cardman Desktop Serial 3111		RS	Vertical Plug&Play smart card reader with RS232 serial interface. Power supply through special PS/2 connector that is connected in the PC mouse/keyboard slot. PC/SC interface support.
	Cardman Desktop USB 3121		USB	Vertical Plug&Play smart card reader with USB interface. PC/SC interface support.

Certificate requirements

To declare taxes online via the portal of the Czech Tax Administration a special software is required that can be downloaded form the web site http://adis.mfcr.cz/adis/jepo/info/provoz_popis.htm.[203]

Application programming interface for online-verification

A lists of revoked commercial certificates as well as a Certification Revocation List of qualified certificates can be found on the website of ICA Certification Authority.

Also PostSignum publishes Revocation Lists:
CRL of the Root Certification Authority:
http://www.postsignum.cz/crl/psrootqca.crl
CRL of the subordinate certification authority:
http://www.postsignum.cz/crl/psqualifiedca.crl

[203] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile The Czech Republic, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

The same hold for the eIdentity CA:
Actual lists of revocated qualified certificates are available in an electronic form in the CRL format on http://www.acaeid.cz/root/crl/actual.crl and http://www.acaeid.cz/aca/crl/actual.crl.

2.5.4 Summary

Table 20 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 20: Summary and rating, The Czech Republic, source: own illustration

categories		rating
legal framework	The EU directive has been adopted in 2000 and the law came into force in 2001.	A
technical standard	eGovernment gateway, eProcurement, eTax advanced eS on qualified SW certificates or qualified certificates on SCs or tokens, SW certificates 3 accredited CSP Smartcards (like DIS) several types of card readers CRL	A
distribution	eGov Gateway: 40.000 users registered, not everyone uses system actually In public procurement, more than 50% of the standard forms were send electronically in the second half of 2006 using advanced electronic signature electronically sent tax returns, 74% are signed with advanced ES, system mainly used for fiscal administration, The overall number of electronically submitted tax declarations that contain an electronic signature is 138.558 forms. Currently the Czech Ministry of Labour and Social Affaires is the only state organisation that uses chip cards in great number	B

2.6 Denmark

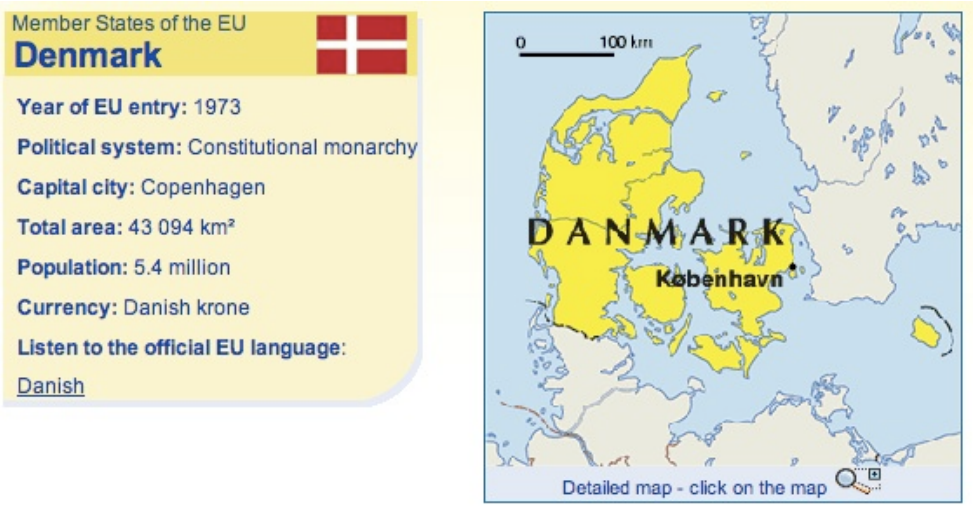


Figure 28: Fact-sheet: Denmark, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:49

In figure 28 some basic demographic and geographic data of the country is presented.

2.6.1 Institutional frame

Legislation

The EU-directive for the general framework for electronic signature was implemented by means of tree national regulations:[204]

1. Law No. 417 concerning electronic signature, 31. May 2000 (see Appendix – Denmark: Law on electronic signatures)[205]
2. executive order No. 999, 5th October 2000, on Reporting of Information to the National Telecom Agency by Certification Authorities and System Auditors - Bekendtgorelse nr. 922 af 5. Oktober 2000 om noglecentres og systemrevisionens indberetning af oplysninger til Telestryrelsen (see Appendix – Denmark: Executive Order on Reporting of Information to the National Telecom Agency by Certification Authorities and System Auditors).[206]
3. executive order No. 923, 5th October 2000, on Security Requirements etc. for Certification Authorities,

[204] cf. Correspondence with Mag. Volker R. Ammann, commercial attaché for Kopenhagen, Federal Economic Chamber, foreign trade office in Kopenhagen

[205] cf. http://www.itst.dk/wimpdoc.asp?page=tema&objno=95025061 , access on 19.07.07, 11: 43

[206] cf. http://itst.dk/wimpdoc.asp?page=tema&objno=95024224 , access on 19.07.07, 11:35

Bekendtgorelse nr. 923 af 5. oktober 2000 om sikkerhedskrav m.v. til neglecentre (see Appendix - Denmark, Executive Order on Security Requirements etc. for Certification Authorities) [207]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Denmark: National Regulations Details.[208]

•recognition of foreign certificates:[209]
In October 1998, the agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of Online Services

•eGovernment:
In January 2001, a citizen portal (http://www.borger.dk) was launched that is operated by state and local authorities. It serves as an entry point to all public authorities and offers services to citizens. [210]

Also an eGovernment portal for businesses (http://www.virk.dk) was implemented that provides a range of fully digital solutions, all in all about 200 eForms.[211] Those forms must be filled out and signed with advanced electronic OCES signatures that are based on software certificates or smart cards.
Currently about 33.00 companies hold an electronic signature and about 4.000 company certificates have been issued.[212]

•ETHICS platform - public procurement:[213]
The platform Electronic Tender Handling, Information & Communications system (http://www.innovasion.dk) includes complex tendering processes and was developed by the Danish

[207] cf. http://www.itst.dk/wimpdoc.asp?page=tema&objno=95024223, access on 19.07.07, 11: 46

[208] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[209] cf. Study of the Donau Universität Krems, Master-Studie, Austria

[210] cf. http://www.epractice.eu/index.php?page=document.print&type=&doc_id=3323&doclng=6, access on 25.08.07, 01:18

[211] cf. http://www.epractice.eu/index.php?page=document.print&type=&doc_id=3323&doclng=6, access on 25.08.07, 01:18

[212] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Denmark, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[213] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Denmark, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

National Procurement LTd. The system relies on a Public Private Key infrastructure based on X-509v.3 standards. Advanced electronic signature based on personal (software) certificates is required.

•TastSelv Borger - eTax:[214]

This system is an automated tax process that is mainly (with 97% of reported data) used by employers, banks, trade unions and different institutions. To log in, a TastSelv code (issued by the Tax Administration) or an advanced digiatl signature based on a software certificate or on smartcards can be used.

The statistic on the total number of logins via PIN and digital signature as well as the number of persons having a login can bee seen in the tables below (table 21, table 22):

Table 21: Number of Logins to TastSelv Borger, source: European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Denmark, April 2007, source: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Country	application	Login method	2004	2005
Denmark	TastSelv Borger	Number of Logins via Pin	2.765.020	3.113.476
		Number of Logins via digital Signature	206.662	487.249
		Total	2.971.682	3.600.726

Table 22: Number of persons with login to TastSelv Borger, source: European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Denmark, April 2007, source: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Country	application	Login method	2004	2005
Denmark	TastSelv Borger	People with Pin	1.148.182	1.259.289
		People with digital Signature	64.379	172.379
		Total	1.212.561	1.431.668

•Sundhed.dk - eHeath portal:[215]

Sunhed.dk is a public health portal that brings together Danish health services on one platform and provides information electronically as well as different eServices.

The user logs in with a digital certificate, differentiation between citizens that access own information and healthcare professional that want to access patient data. Currently about 110.000 users are registered with certificates but only pilot projects are running to validate the exchange of certificates between different systems.

[214] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Denmark, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[215] cf. Number of persons with login to TastSelv Borger, source: European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Denmark, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•other eServices:
All operational and planned eGovernment applications are listed up in the Appendix - Denmark: Operational and planned applications.[216]

Types of electronic signature

The Danish Central Customs and Tax Administrates designed the first internet based solution in 1994. It included a Pin code entry and encryption technique. This solution is basically the same as used today.[217]

In 2003, the Danish government has developed an official electronic signature scheme: It provides all citizens with a free electronic signature, that can be used for the most public and private contacts (see also http://www.digitalsignatur.dk).[218]
The Central Customs and Tax Administration planned to provide all citizens with digital signatures, starting with issuing 350.000 certificates in 2003 and to increase the number over the next four years. The Administration aims to improve the communication for citizens and businesses, including the use of digital signature for all services of the Administration.[219]

For electronic tax declarations a total number of 1.431.668 users were registered in 2005 for the eTax system, 172.379 of them having a digital signature login.[220]

For advanced electronic signature, a Danish standard has been developed (see also http://www.signatursekretariatet.dk/certifikatpolitikker.html)[221], the so called OCES signatures.

The Certification Service Provider TDC delivers the basic technology to the public sector and so establishes closer links between the government and the citizens. TDC has an agreement with ToldSkat, the Central Customs and Tax Administration, to issue digital signature via the online ordering service. The digital signature is the digital proof of identity of the citizens and can be used to communicate with public authorities and private companies. More and more online services furnish grater flexibility as the user can log in and make his transactions when- and wherever he wants. The Government has ensured free certificates for all citizens.[222] The signature is used, for example, for electronic tax filling and should enable

---

[216] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[217] cf. Nielsen, Jeannette, Meinertz, Ulrik, Denmark Launches Nationwide Digital Signatures, March 2003

[218] cf. Correspondence with Mag. Volker R. Ammann, commercial attaché for Copenhagen, Federal Economic Chamber, foreign trade office, Copenhagen

[219] cf. Nielsen, Jeannette, Meinertz, Ulrik, Denmark Launches Nationwide Digital Signatures, March 2003, http://www.centerdigitalgov.com/international/story.php?docid=43522, access on 14.11.2007, 20:04

[220] cf. Number of persons with login to TastSelv Borger, source: European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Denmark, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[221] cf. Correspondence with Charlotte Jacoby, National IT and Telecom Agency, Copenhagen

[222] cf. http://tdc.com/publish.php?id=2419, access on 22.07.07, 11:17

citizens to undertake all their business with public authorities from their computers at home in a secure way.[223]

But the implementation of digital signatures proceeded very slowly, as there was neither demand nor supply. The Government was faced with many barriers. A key barrier was that people only create trust, when people how up in person and verify their identity. Also people had no motivation to demand digital signature as it is linked with an investment in hardware (smart cards, smart card readers).[224]

Also, no qualified electronic signatures (advanced electronic signatures based on qualified certificates and created by a SSCD) are offered in Denmark. Currently, there is no need for such a type of signature.[225]

2.6.2 Application requirements

Types of certificates

Currently the main focus is on the above mentioned OCES signatures.

There are 3 types of certificates available:

- personal certificates
- employee certificates
- company certificates.[226]

Currently about 33.00 companies hold an electronic signature and about 4.000 company certificates are issued.[227]

Qualified certificates are not issued in Denmark at the moment. Most of the advanced security solutions based on qualified certificates are not technologically developed enough. The price of these ones that are of a high technological standard is too high to make them practically accessible to most people.[228]

In Denmark are only software certificates are available[229], namely the OCES certificates are software - based and non-qualified[230] with use of password.

---

[223] cf. Nielsen, Jeannette, Meinertz, Ulrik, Denmark Launches Nationwide Digital Signatures, March 2003

[224] cf. Nielsen, Jeannette, Meinertz, Ulrik, Denmark Launches Nationwide Digital Signatures, March 2003

[225] cf. http://www.epractice.eu/index.php?page=document.print&type=&doc_id=3323&doclng=6, access on 25.08.07, 01:18

[226] cf. http://www.signatursekretariatet.dk/certifikatpolitikker.html, access on 22.07.07, 11:02

[227] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Denmark, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[228] cf. National Association of Local Authorities in Denmark et al, Digital Administration, Mai 2001

[229] cf. Correspondence with Charlotte Jacoby, National IT and Telecom Agency, Copenhagen

[230] cf. http://www.itst.dk/publikationer-uk/annual_report_2004/annexes/html/chapter02.htm, access on 22.07.07, 11:25

For more technical details of OCES see Appendix - Denmark, Technical details of OCES.

The Danish Ministry distributes documents from the European Council by the Internet. This is done by using IDGate, a digital certificate solution of TDC Internet. This solution ensures access control to web servers by means of digital certificates. Only authorized persons have access to the documents as IDGate identifies users. At the same time, the solution can encrypt the communication between the users' workstation and the Council's web-server.

User certificates can be issued to everyone the company wants to give access to the web-servers, as employees, customers or cooperation partners.

The certificate enables a „two factor identification" of the user with the personal encryption key and the personal activation code that the user knows. The IDGate solution is part of the offering from TDC Internet developed for E-Government.[231]

Certification Service Providers

In Denmark there is only one Certification Service Provider that issues these OCES certificates the TDC Certificeringscenter[232], as DMdata and Eurotrust have stopped to work as CAs.[233]

➡Short description: TDC Certificeringscenter[234]:

TDC was a traditional provider of mobile and landline services in Denmark and has developed to the leading provider of communication solutions.

Table 23 lists up all certification service providers in Denmark.

Table 23: Certification Service Provider in Denmark, source: own illustration

Certification Service Provider		Issued Certificates
TDC Certificeringscenter		OCES certificates - personal certificates - employee certificates - company certificates = software-based = non-qualified with Pin-entry

[231] cf. http://tdc.com/publish.php?id=2409, access on 22.07.07, 11:16

[232] also see http://www.tdc.dk or http://www.certifikat.dk

[233] cf. http://www.itst.dk/publikationer-uk/annual_report_2004/annexes/html/chapter02.htm, access on 22.07.07, 11:25

[234] cf. http://tdc.com, access on 22.07.07, 11:11

Inspecting authorities

The Certification Service Provider TDC is observed by the National IT and Telecom Agency. If a CA wants to issue OCES certificates, it must have an agreement with the National IT and Telecom Agency. The CA must observe the terms of the certificate policy and submit an annual report to the National IT and Telecom Agency.

2.6.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

There is no secure signature-creation device recommended or supported by TDC.[235]

In Denmark, eGovernment applications like TastSelv Borge, Virk.dk or Netborger.dk can be accessed, using smartcards or software certificates.[236]

Card readers

A secure Pin-entry is not applicable[237] as no advanced electronic signature is offered in Denmark.[238]

Certificate requirements

The required software for the OCES signatures is issued by TDC and developed for all standard operating systems.[239]

Application programming interface for online-verification

Online lists of revoked certificates are provided.[240]

---

[235] cf. Correspondence with Charlotte Jacoby, National IT and Telecom Agency, Copenhagen

[236] cf. European Commission, IDABC, Token Type, http://ec.europa.eu/idabc/en/chapter/6004, access on 23.11.2007, 13:32

[237] cf. Correspondence with Charlotte Jacoby, National IT and Telecom Agency, Copenhagen

[238] cf. http://www.epractice.eu/index.php?page=document.print&type=&doc_id=3323&doclng=6, access on 25.08.07, 01:18

[239] cf. Correspondence with Charlotte Jacoby, National IT and Telecom Agency, Copenhagen

[240] cf. Correspondence with Charlotte Jacoby, National IT and Telecom Agency, Copenhagen

2.6.4 Summary

Table 24 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 24: Summary and rating, Denmark, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2000. Danish official electronic signature scheme, Danish standard for advanced electronic signature,	A
technical standard	eGovernment portal, about 200 eForms, require OCES signatures eProcurement, eTax, eHealth first internet base signature solution in 1994 (still the same), Danish standard for advanced eS: OCES signatures (advanced eS on SW, SC) most certificates on software token no qualified certificates on SSCD, as they are not technologically developed enough only 1 CSP Smartcards or SW token cardreaders without secure PIN-entry CRL	C
distribution	Implementation of digital signature very slowly as there is neither demand nor supply, little motivation to invest in hardware. Currently about 33.000 companies hold eS, about 4.000 company certificates have been issued. The total number of users that are were registered in 2005 for the eTax system is 1.431.668, 172.379 of them having a digital signature login. About 33.00 companies hold an electronic signature and about 4.000 company certificates are issued No qualified eS, as there is no need for it	B

2.7 Estonia

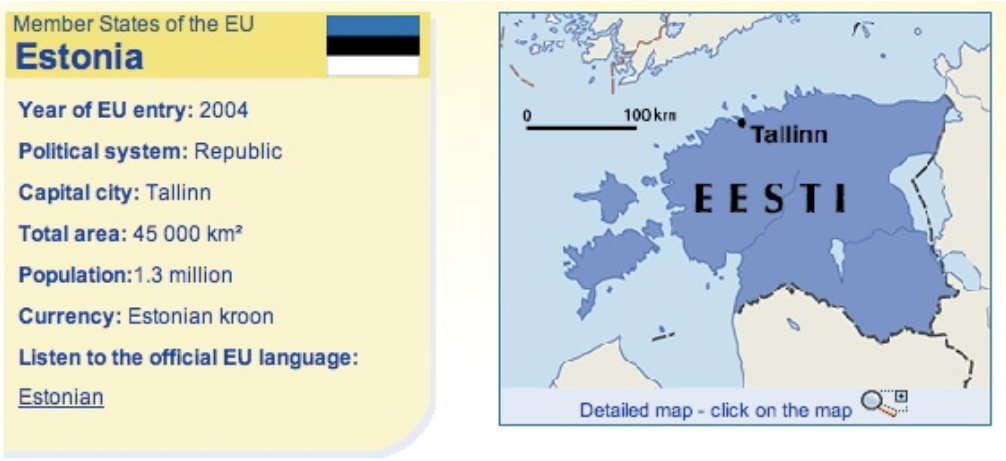


Figure 29: Fact-sheet: Estonia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:50

In figure 29 some basic demographic and geographic data of the country is presented.

2.7.1 Institutional frame

Legislation

The Digital Signature Act (see Appendix – Estonia: Digital Signature Act) was passed on the 8th of March 2000 and entered into force on the 15th of December in the same year.[241]

The Digital Signature Act regulates only advanced electronic signatures. According to the act, digital signatures are equal to handwritten signatures. The Act also states, that public sector authorities have to accept digitally signed documents. Other types of electronic signatures are not regulated by the act. The signatures can be used but do not have legal power.[242]

In 2003, Estonia and Finland signed an agreement for harmonizing the application of digital signature, document format and exchange. Concepts and practices should be standardized[243].

[241] cf. Correspondence with Tarvi Martens, Development Director, The Certification Centre SK, Correspondence with Johannes Brunner, commercial attaché for Finland, Estonia, Latvia and Lithuania, Federal Economic Chamber, foreign trade office, Helsinki

[242] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Estonia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[243] cf. Höpner, Petra, Study PKI and Certificate Usage in Europe 2006, Fraunhofer Institute FOKUS, 2006

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Estonia: National Regulations Details.[244]

•recognition of foreign certificates:[245]
The Estonian Digital Signature Act regulates the mutual recognition of foreign electronic certificates. To be recognized, the foreign certificate must be confirmed by an Estonian certification service provider and be compliant with legal requirements or be covered by any international agreement. But up to now, there has not been any practical need for accepting foreign certificates in the public sector.

Availability of online services

•eGovernment applications:
Most of the eGovernment applications use electronic signatures. Government employees use no special certificates beside the ID-cards. A lot of public tools (like DigiDoc) are used to create and handle electronic files. Some systems have been developed web applications that include digital signing capability, either by DigiDoc software libraries or web services. Examples for such systems include:

- „Citizenship and Migration Bureau – system for internal document handling, on-line applying for ID documents (requires electronic signature)
- Ministry of Justice, Centre of Registers and Infosystems – electronic submission of annual reports of a company and foundation and lists of the members of a political parties http://www.eer.ee/el_esit_eng.phtml
- Tax Board – webservice for submitting arbitrary digitally signed documents https://apps.emta.ee/digireg/index.jsp
- Portal for submission of digitally signed e-forms to various municipal and governmental organizations (approximately 60 institutions are joined) – www.eesti.ee
- Patent Bureau – service for applying for a trademark (planned)
- Minstry of Justice – incorporation of companies online using ID-card and digital signature – registration shall be handled in 2 hours from 01.01.2007.“[246]

•eTax:
The Tax Board added a digital signing option to its homage. The user can upload his tax documents into the data management system and these documents are certified by digital signature.

•DigiDoc:
In 2002, a basic platform for digital signature was developed in Estonia: DigiDoc. It includes a client program and a portal for the end-user. Many people have used this platform and have given very important feedback to the developers, concerning improvement or supplement of certain options.

---

[244] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[245] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Estonia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[246] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Estonia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

In 2003, the DigiDoc software was extended by the possibility of digital stamps of agencies (digital verification). This application enabled the certification of authorization of an individual that has signed digitally and made the use of e-certificates possible. Additionally, it automatically certifies extracts from registers. Figure 30 shows the main page of the platform.

Figure 30: DigiDoc platform, source: http://www.digidoc.com/, access on 22.08.2007, 12:05

•eVoting:[247]

During municipal elections in Estonia in October 2005 Internet-based voting was used and applied countrywide. The legislative framework was created in 2002, thereafter the National Electoral Committee launched a project to develop the eVoting system in 2003. The electronic voting was enabled by the ID cards. Exactly 9.317 voters made use of the new system and voted electronically, 9287 votes were valid out of 850.000 eligible voters holding the ID card.

•other eServices:

The Ministry of Justice started introduction and training project to enable reading e-documents that are digitally signed and exchanging them with lawyers. In Health Insurance, the ID card replaces the health insurance Card.

The Police use the ID card, inspects the database and so verifies the driver-license, car registration or traffic insurance.[248]

[247] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Estonia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[248] cf. http://www.riso.ee/en/pub/2003it/p32_s.htm , access on 21.007.2007, 10:44

Types of electronic signature

In Estonia, just advanced electronic Signature in terms of the Directive is issued.[249]

Many public administration agencies have started use digital signature.
The Tax Board, for example, added a digital signing option to its homage. The user can upload his tax documents into the data management system and these documents are certified by digital signature.
Also the Ministry of Justice have successfully implemented digital signature. On 12 June 2003, digital signature was fist accepted as evidence to handwritten signature. The Ministry of Justice started introduction and training project to enable reading e-documents that are digitally signed and exchanging them with lawyers. In Health Insurance, the ID card replaces the health insurance Card.
People will no longer need to take around all documents with them. The Police use the ID card, inspects the database and so verifies the driver-license, car registration or traffic insurance.[250]

Electronic signature is widespread in Estonia, it can be used by almost everyone. A lot of businesses use it, but citizens also have taken interest in the service.[251]
Currently, 88.883 persons gave signed digitally using an ID card.[252]

2.7.2 Application requirements

Types of certificates

The ID-card is provide with two certificates, one for personal identification and on for digital signing. It contains some personal data, like your name and the personal identification code. When an user signs a document digitally, his signature must be verified. The program for issuing digital signature automatically contacts the web server of the Certification Centre SK to verify the validity of this certificate. In caste that the certificate is valid, the server issues a warrant that is attached to the signature.[253]

The ID card contains two types of certificates: one for authentication and another for digital signing. These qualified certificates follow the X.509v3 Standard and are issued by SK. The fields of the certificates for signature are described in detail in the Appendix - Estonia: Fields of the signature certificate of the Estonian ID Card. For more technical detail see Appendix – Estonia: Estonian EID certificate profile.

Issuing a digital signature as well as their verification is convenient with the DigiDoc system.

---

[249] cf. Correspondence with Tarvi Martens, Development Director, The Certification Centre SK, Correspondence with Johannes Brunner, commercial attaché for Finland, Estonia, Latvia and Lithuania, Federal Economic Chamber, foreign trade office, Helsinki

[250] cf. http://www.riso.ee/en/pub/2003it/p32_s.htm , access on 21.007.2007, 10:44

[251] cf. Correspondence with Ülar Kaldasaun, Numbering Managing Department, Specialist, Estonian Technical Surveillance Authorty, Estonia

[252] cf. Correspondence with Tarvi Martens, Development Director, The Certification Centre SK

[253] cf. http://www.id.ee access on 21.07.2007, 12:12

Personal software certificates are not delivered.[254]

The Certification Center SK provides all kinds of certificates. For natural persons, it issues qualified certificates only on secure signature-creation devices, like on ID card or on MobileID.
At the moment, 2 x 1.188.116 certificates have been issued for ID cards (2 certificates per card), with 999.030 cards being active, 2 x 4.804 certificates have been issued for MobileID. [255]

Certification Service Providers

Currently, there is only one certification service provider operating in Estonia, and two functioning timestamping service providers.[256]

The Certification Centre (SK) was founded in February 2001 by EMT, Eesti Telefon, Hansabank and the Union Bank and is an accredited provider of certificates and time-stamping services.

•Short description: The Certification Centre SK[257]
SK is a Certification Service Provider that was stately accredited. It is the primary and currently only certification authority that provides certificates to Estonian ID cards for digital signing and authentication.
The services of SK include the software development for certification and time-stamping as well as development of ticket and payment systems.[258]
But the main function is to ensure the integrity and reliability of the Infrastructure behind the project of the ID cared project.[259]

Table 25 lists up all certification service providers in Denmark:

Table 25: Certification Service Provider in Estonia, source: own illustration

Certification Service Providers		Issued certificates
The Certification Centre SK	SK	advanced electronic signature

Inspecting authorities

The Communication Board observes the CSPs.[260]

[254] cf. Correspondence with Tarvi Martens, Development Director, The Certification Centre SK

[255] cf. Correspondence with Tarvi Martens, Development Director, The Certification Centre SK

[256] cf. Correspondence with Ülar Kaldasaun, Numbering Managing Department, Specialist, Estonian Technical Surveillance Authorty, Estonia

[257] cf. http://www.sk.ee, access on 24.07.2007, 08:45

[258] cf. http://www.id.ee access on 21.07.2007, 12:12

[259] cf. http://www.sk.ee, access on 24.07.2007, 08:45

[260] cf. Correspondence with Tarvi Martens, Development Director, The Certification Centre SK

2.7.3 Technical preconditions

Signature software

n.a.

Types of secure signature-creation device

The Certification Authority SK offers chip cards as they are the most secure tokens.[261]

•ID card:

On the 1st of January 2002, the first ID cards were issued in Estonia.

These IDcards were issued by the Estonian Citizenship and Migration Board for Estonian citizens and for foreigners that reside in Estonia with a residence permit.[262]

By the end of 2003 already 350,00 ID cards had been issued to Estonian citizens, which means nearly 25% of the whole Estonian population). In October 2002, the first digital signature was created.[263]

By the end of May 2004,nearly 500.000 ID cards had been issued (including 83.141 ID cards for foreigners).[264] By February 2006, over 900.000 ID cards had been issued, this means to 61% of the Estonian population.[265] By the end of 2007, almost all citizens will have received an ID card.[266]

Id cards can be used for electronic identification and for creating digital signatures. It also serves as an ID document for Estonian residents over the age of 15. Additionally the card is an identification and travel document within the European Union, valid for 10 years. An electronic processor chip on the ID card records a personal data file, the certificate for authentication and a certificate for creating digital signature.[267]

The ID card can be used

- for personal identification over the Internet,
- for creating digital signature,
- for encryption,

---

[261] cf. http://www.sk.ee, access on 24.07.2007, 08:45

[262] cf. http://www.ria.ee, access on 21.07.2007, 21:56

[263] cf. http://www.riso.ee/en/pub/2003it/p32_s.htm, access on 21.07.2007, 10:44

[264] cf. Jaak Tepandi, Arvo Ott, eSecurity activities 2004, Presentation, SOIS meeting, 01.10.2004

[265] cf. http://www.ria.ee, access on 21.07.2007, 21:56

[266] cf. Jaak Tepandi, Arvo Ott, eSecurity activities 2004, Presentation, SOIS meeting, 01.10.2004

[267] cf. http://www.ria.ee, access on 21.07.2007, 21:56

- for electronic voting and[268]
- to access different services, for example the DigiDoc platform.

•Mobile ID service:
The Estonian Certification Center and EMT, a high technology service company in the telecommunication and information sector, have launched a Mobile-ID service that enables customers to identify themselves via their mobile phone. The SIM has added functionality, the client gets the usual keys (Pin, PUK) and additional codes for online identifications and for creating a digital signature.
The User can log onto an Internet-banking system for example and will be identified.
This service is available for the clients of EMT and the exchange of the SIM card is free of charge until the end of 2007. Thereafter, an exchange will cost the usual price and the service of Mobile-ID will cost a monthly fee of 10 kroons.
The service needs to be activated at the website www.id.ee with use of the ID-card, a card reader and its Pin-code.[269]

Card readers

Now, the first ID card readers for notebooks are available in Estonia. So, customers of the Estonian Bank can now use their ID cards to log into the bank's system and manage their transactions online.

Recommended card readers are listed up in table 26:

Table 26: Recommended card readers, source: http://www.id.ee, access on 21.07.2007, 12:12

Provider	Mark (Model)		Connection	Provided Operating System
Omnikey	Omnikey CardMan 4040		PCMCIA	Windows 98/ME Windows 2000 Windows XP Windows Server 2003 Windows XP64bit (IA64, AMD64, EM64T) Windows Vista 32bit Windows Vista 64bit Windows CE (depending on hardware) Linux Mac OS X
	Omnikey CardMan 4321 ExpressCard 54		PCCard	Windows 98/ME Windows 2000 Windows XP Windows 2003 Server Windows XP64bit (IA64, AMD64, EM64T) Linux

[268] cf. http://www.id.ee, access on 21.07.2007, 12:12

[269] cf. http://www.id.ee access on 21.07.2007, 12:12

These models are compatible with most PC notebooks and can be used with Windows or Linux operating systems.

Also extern card readers with USB connection can be used. [270]

The greatest distributors of external card readers ate at the moment K-Arvutisalong, Elion, Hansabank and SEV Eesti Uhisbank are the greatest distributors [271]

The Certification Centre SK recommends smartcard readers with Pin-pads for public places. But for price reasons, people are still buying regular smartcard readers for about 6€.[272]

Certificate requirements

For the use of the ID card, various software is demanded. The complicated software installation raised some problems. Software needed to be installed, like drivers for the card reader and for the ID card, the DigiDoc client program, and everything in correct order. For the common user, this turned out to be quite difficult.

Therefore, AS Sertifitseerimiskeskus and SA Vaata Maailma developed a special ID card installation software for the Windows platform. With help of this software, installation became less complicated.

Also an ID card starter set was offered by the end of 2003, including the ID card installation software, the card reader and a manual for easy setup.[273]

The ID-card software was fist only available for Windows platforms and usable with the Internet Explorer web browser. Now the software also supports Mozilla Firefox web browser. The user can also sign e-mails digitally or encrypt mails with Mozilla Thunderbird.[274]

DigiDoc Client needs to have access to an OCSP responder. [275]

Application programming interface for online-verification

The Certification Centre SK enables verification of digital signatures with the DigiDoc system. The Program automatically contacts the web-server of SK and proofs the validity of the certificate. If it is found valid, the server issues a warrant that is attached to the signature.[276]

---

[270] cf. http://www.id.ee, access on 21.07.2007, 12:12

[271] cf. http://www.id.ee, access on 21.07.2007, 12:12

[272] cf. Correspondence with Tarvi Martens, Development Director, The Certification Centre SK

[273] cf. http://www.riso.ee/en/pub/2003it/p32_s.htm, access on 21.007.2007, 10:44

[274] cf. http://www.id.ee, access on 21.07.2007, 12:12

[275] cf. http://www.sk.ee, access on 24.07.2007, 08:45

[276] cf. http://www.sk.ee, access on 24.07.2007, 08:45

2.7.4 Summary

Table 27 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 27: Summary and rating, Estonia, source: own illustration

categories		rating
legal framework	In 2000 a digtial signture act was passed and came into force in the same year. Act only regulates advanced electronic signatures, no ohter eS are regulated and tuhs have no legal power. 2003, agreement with Finland, harmonisation of application document format and exchange	B
technical standard	eGov, Platform for eS: DigiDoc, eTax, eVoting project only advanced eS First eID cards in 2002, DigiDoc platform, eGov, eTax, eVoting mobile SIM ID, ID card The Certification Centre Sk recommends card readers with PIN Pads, but people buy regular readers for price reasons. OCSP service	B
distribution	most eGov applications use eS eVoting project: 9.317 votes by eID card (out of 850.000) eS widespread in Estonia, lot of businesses use it, also citizens have interest in it By 2006, 61% of the Estonian population owned an eID card (over 900.000 IDcards) Currently, 2x1.188.116 certificates have been issued for eID (2 certificates per card)	A

2.8 Finland

Figure 31: Fact-sheet: Finland, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:50

In figure 31 some basic demographic and geographic data of the country is presented.

2.8.1 Institutional frame

Legislation

The EU-signature-directive was implemented on the 1st of February 2003. On this day, the law and both Regulations came into force (see Appendix - Finland: Act on Electronic Signature, and Appendix – Finland: Regulations).

In 2003, Estonia and Finland signed an agreement for harmonizing the application of digital signature, document format and exchange. Concepts and practices should be standardized[277].

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Finland: National Regulations Details.[278]

[277] cf. Höpner, Petra, Study PKI and Certificate Usage in Europe 2006, Fraunhofer Institute FOKUS, 2006

[278] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•recognition of foreign certificates:[279]
In March 1998, an agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:
Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of Online Services

•eGovernment:[280]
In Finland, the government is responsible for defining long-term visions and strategies to provide a general mission statement for eGovernment. The coordination is driven by

- the Ministry of Finance, that coordinates all eGovernment actions,
- the Ministry of the Interior, that manages all information in regional administration as well as local authorities,
- the Ministry of Justice , that takes law-making initiatives for providing eGovernment services and setting a main regulatory framework and
- independent agencies like the Finnish Social Insurance Institution KELA, that is under parliamentary authority.

The use of electronic signatures on basis of a qualified certificate is not wide spread in eGovernment applications, the use of the FINEID signature is only optional.

•Public Procurement:[281]
Finnish online procurement notification as well as database services do not support FINEID or digital signatures and relies in most cases on simple username-password authentication mode.

---

[279] cf. Study of the Donau Universität Krems, Master-Studie, Austria

[280] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[281] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•Public services on Lomake.fi:[282]
On Lomake.fi, the Ministry of Finance offers a large amount of applications and electronic forms for multiple purposes. Those can be either downloaded and printed or pre-filled and submitted via Internet, requiring authentication by using FINEID or TUPAS (see Chapter Finland - Types of certificates).Lomake.fi was launched in 2002 and offer forms and applications of organizations like the Vehicle Administration, National Social Security, Municipalities, different ministries, Tax Administration, FICORA and more.
To use the services a FINEID signature is required on FINEID card but also a TUPAS one time password can be used. But most people are freely accessible for download, printed and hand signed, only 0.2% of this services are signed with FINEID.

•Epoline eOLF - Patents online service:[283]
This service enables to fill patent applications electronically and is provided by the European Patent Office. Electronic Patent applications that are addressed to the National Board of Patents and Registration of Finland need to be signed with a FINEID Citizen Certificate or an Organizational Card, applications of the European Patent Office can be signed with an EPO Smart card (with advanced electronic signature certificate).
Approximately 40% of the national applications or forms are received electronically.

•TEKES online services:[284]
The Finnish Funding Agency for Technology and Innovation (Tekes) was one of the first Finnish organistaion that adopted XML signature technologies. Tekes funds over 2.000 project annually, particularly R&D projects and projects of university or research institutes. On the website www.tekes.fi, application forms are available that can be signed electronically using FINEID card or TUPAS one-time password. As the forms can also be submitted without using electronic signatures, the signature function is not used very often.

• TYVI Pro service - electronic declarations:[285]
TYVI Pro is an A2B broker system, launched in 1997 and operated by Elma Oy. Different Authorities can offer electronic forms for VAT declarations, payroll tax reports etc.
The portal can be reached with an user ID and a password (TUPAS) or using a FINEID card. Around 0,2% of this services are accessed using FINEID.
Already 120.000 companies report information via TYVI which matches it to Finland‘s most used eGovernment portal.

---

[282] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[283] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[284] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[285] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

A range of applications are operating or planned in Finland and are listed up in the Appendix - Finland: Operational and planned applications in detail.[286]

Types of electronic signature

In Finland the following types of signatures are used:[287]

- advanced electronic signature
- qualified electronic signature, based on qualified certificates, created by a secure signature creation device. The qualified signature is legally equivalent to a handwritten signature.

2.8.2 Application requirements

Types of certificates

•Citizen Certificate:

is an electronic identity that contains information about the citizens (like the name) and an electronic client identifier.

The electronic identity is created by providing the citizens with a personal identity code. The electronic client identifier identifies the electronic user in secure online transactions. The certificate is used for identification, encryption of e-mails, data or documents and for providing electronic signature.[288]

This Citizens Certificate can be attached to the ID card, the Visa Electron card that is issued by the Finnish OP Bank Group or to a mobile SIM card.[289]

- Citizen Certificate on ID card:
  The ID card is embedded with a chip that contains the Citizen Certificate. With help of this certificate a person can be identified when using online services. It helps the services user and the provider authenticate each other's identity.
  You can also have your e-mail address saved on the ID card, which increases the usability with email-software.
  The ID cards are issued by the Police. It costs 40€ and is valid for five years. The ID card serves as a valid travel document and replaces the passport.
  Since the 1st of June 2004, the ID card can be combined with the national health insurance card

---

[286] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[287] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[288] cf. http://www.vaestorekisterikeskus.fi/crk/home.nsf/www/electronic identity, access on 25.07.2007, 9:10

[289] cf. http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/9C0B5FFC32EC6AF2C225724400511298?opendocument, access on 25.07.2007, 9:12

(Kela card).[290]

By the end of July, already 153.600 Citizen Certificates had been issued.[291]

- Citizen Certificate on bank card:

  For customers of OP Bank Group‘s member banks the Visa Electron payment card can be provided with an Citizen Certificate. With use of an PIN code it is possible to make secure transactions at some online services, like the OP Bank Group‘s Internet bank. But as bank cards can not provide photos, the bank card can not replace the passport or the Kela card.

- Citizen Certificate on mobile phone SIM card:

  The Citizen Certificate can also be implemented onto a SIM card of a mobile phone. The customer can now use his mobile phone as an identification and digital signature tool. The mobile phone replaces the computer card reader.

  This kind of certificate is qualified.

  In November 2004, the Population Register Centre agreed an cooperation with the telecoms operator TeliaSonera Finland Oyj. Also Elisa Cooperation, another telecoms operator, issues its SIM cards with a qualified certificate since June 2005.

  Another cooperation is underway with DNA Finland Ltd.[292]

The Fields of the FINEID citizen signature Certificate are described in Appendix - Finland: Fields of FINEID Citizen Signature Certificate.[293]

•E-mail certificate:

An organization (a business unit or department) has an individual e-mail address that is monitored by several people. Such e-mail addresses are used for transmitting registrars, orders, notifications or operation requests. Using the certificate, encrypted messages can be opened. Messages that are sent out can also be signed digitally.

This e-mail certificate is only file-based, so no card reader or further software is needed and works for the most e-mail software that supports S/MIME messages.[294]

•Organization Certificate:

The Population Register Centre also issues organization cards to companies that store certificates. This card is used for verification of a person‘s position or customer-ship. It is also possible to issue an electronic signature and to authenticate network users and their access rights.

---

[290] cf. http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/A0D3A8D03E6882C5C225724400 5213EC?opendocument, access on 25.07.2007, 9:13

[291] cf. http://www.fineid.fi/en, access on 18.08.2007, 12:32

[292] cf. http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/FE039B4246B8FED9C225724500 36E7E6?opendocument, access on 25.07.2007, 09:16

[293] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[294] cf. http://www.fineid.fi/vrk/fineid/home.nsf/pages/C3B39DB2DB61D6B7C2257054002DB718, access on 25.07.2007, 09:17

Also the organizations e-mail address an be included in this certificate to sign and encrypt e-mails or loin in to the organizations network.

An organization has the possibility to design the organization cards in accordance with the general graphic image of that organization by using colors of placing logos. The Cards can also include photos or a blank space for a signature of the cardholder (figure 32).

Figure 32: Organization cards, source: http://www.fineid.fi/vrk/fineid/home.nsf/pages/CBFA42967D2B705AC2257054002DB66F, access on 25.07.07, 9:32

•Server Certificate:[295]

The Server Certificate allows to identify a service provider, both in the public and in the private sector. The User of a on-line service can verify the authenticity of the provider. The communication between the browser and the server is SSL-protected.

This kind of certificate can be issuer for one or for two years. The certificate uses key pairs, witch are created by the server administrator, and can be 512, 1.024 or 2.048 bits long.

The Certificates are used to implement three different types of on-line services:

- "server-only certificate": the pages of a web-service use protected communication, the server certificate is bought by the service provider and installed on the server and the user's browser, a user ID and password are utilized,
- "server certificate and user certificate", non-predetermined users: also users receive a certificate, a non-predetermined user base is implemented, provides a strong user authentication.
- "server certificate and user certificate", predetermined users: same as above, but user certificate will be linked to a user ID and user rights.

For more specific detail of the tree types of on-line services see http://www.fineid.fi.

The Finnish eGovernment use tree different types of electronic signature applications:

- Signature applications using qualified certificate on the FINEID electronic ID card
- Signature applications for organizations using qualified certificates („organization CA certificates") on the FINEID certificate card
- TUPAS bank identification system.

[295] cf. http://www.fineid.fi/vrk/fineid/home.nsf/pages/105C03AFB213C30EC2257054002DB6E2, access on 25.07.2007, 09:49

FINEID certificates are qualified certificates according to the EU directive and the Finnish ACt on electronic signatures.
Advanced electronic certificates are not used for eGovernment services.
The TUPAS system does not use qualified or advanced signatures but authenticates uses via a two-factor password.[296]

Certification Service Providers

There is only one Certification Service Provider in Finland: the Population Register Centre (PRC).[297]

➡Short description: Population Register Centre PRC[298]

The PRC was founded in 1969 and operates under the Ministry of the Interior. Its services include the offer of personal and building data services as well as identification solutions fro online-services and certificate services. The Centre is also responsible for the maintenance of the Population Information System, the guardianship register and the Public Sector Directory Service.

Currently, PRC is the only CA that issues qualified certificates in Finland (table 28).

Table 28: Certification Services Providers in Finland, source: own illustration

Certification Service Provider		Issued Certificates
Population Register Centre http://www.vaestorekisterikeskus.fi/	Väestörekisterikeskus Befolkningsregistercentralen	qualified certificates: - Citizen certificate - E-mail certificate - Organization certificate - Server Certificate

Inspecting authorities

FICORA supervises the Certificate Services Provider, Data Ombudsman supervises the handling of personal information.[299]

➡Short description: FICORA

FICORA stands for Finnish Communications Regulatory Authority.
FICORA supports general help concerning information security issues, controls all activities in Finland concerning radio frequencies and licenses for radio devices. It also serves as a regulation authority,

[296] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[297] cf. Correspondence with Johannes Brunner, Austrian Embassy - Commercial Section, Federal Economic Chamber, foreign trade office Helsinki

[298] cf. http://www.vaestorekisterikeskus.fi/vrk/home.nsf/www/about, access on 25.07.2007, 9:10

[299] cf. Correspondence with Johannes Brunner, Austrian Embassy - Commercial Section, Federal Economic Chamber, foreign trade office Helsinki

ensuring that the market competition is effective and companies regard statutory obligations (pricing, operations).[300]

➡Short description: Data Ombudsman
The Data Protection Ombudsman along with the Office of the Data Protection Ombudsman offers guidance and advice on all activities concerning the processing of personal data. and controls the observance of the law.[301]

2.8.3 Technical preconditions

Signature software

n.a.

Types of secure signature-creation device

•The Finnish e-ID card FINEID:
FINEID was created to replace the traditional citizen card. The roll out started on the 1st December 1999. The card served as an ID card for civil servants for identification and authentication services in ministries, agencies and municipalities. The target was that by 2008 the cards should be used by minimum 35 % of the population (around 1,7 million citizens).
The FINEID card is also issued for general citizen use by the local police department. Since 2003, the card is available only as electronic FINEID version. The costs amount to 40€ for the card, the validity of the certificate is 5 years. The plan is to make FINEID citizen cards exempt from charges from 2008.[302]
The ID card, containing a Citizen Certificate, can be used for identification, Encryption of data and e-mails and for issuing digital signature.[303]
The FINEID card is produced by Gemalto (Setec).

•FINEID certificate on SIM:[304]
The FINEID certificate can also be on a SIM card used in mobile phones. The sim card enhanced with this function is called a „SIM Wireless Identity Module“. By SMS or WAP services authentication and digital signature can be achieved. To use the FINEID across carriers, a global roaming service was established by wireless telecommunications service providers.

---

[300] see http://www.ficora.fi/en/

[301] cf. http://www.tietosuoja.fi/1560.htm, access on 25.07.2007, 12:02

[302] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[303] cf. http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/A0D3A8D03E6882C5C22572440 05213EC?opendocument, access on 25.07.2007, 09:15

[304] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Card readers

To be able to use the ID card and make online transaction you need a card reader and an applicable software. When buying an ID-card at the police station, the software is included in the price and can be downloaded from www.fineid.fi/en. On this site also some information about card readers and the certificates is available.[305]

The Population Registry Center recommends the following smart card readers (table 29):

Table 29: recommended smart card readers, source http://www.fineid.fi/vrk/fineid/home.nsf/Pages/0A87A6D1BD836110C2257054002E0773, access on 18.08.2007, 12:40

provider	Model	Type	Driver version	Win 98	Win ME	Win NT 4.0 *	Win 2000 Pro	Win XP Pro
ACS Advanced Card Systems www.acs.com.hk	ACR30U	USB		OK / 2.10.1	OK / 2.10.1		OK / 2.1.0.1	OK / 2.1.0.1
	ACR38U	USB		OK / 1.01.4	OK / 1.01.4	OK / 1.0.0.1	OK / 1.1.4.0	OK / 1.1.4.0
	CCID	USB		OK / 1.1.5.1	OK / 1.1.5.1		OK / 1.1.5.1	OK / 1.1.5.1
	ACR38F	USB		OK / 1.01.4	OK / 1.01.4		OK / 1.1.4.0	OK / 1.1.4.0
	ACR38K	USB		OK / 1.01.4	OK / 1.01.4		OK / 1.1.4.0	OK / 1.1.4.0
	ACR91	PCMCIA		OK / 1.1.0.15	OK / 1.1.0.15	OK/ 1.1.0.15	OK / 1.1.0.15	OK / 1.1.0.15
ActivCard www.activcard.com	ACTR-01	RS/ PS2		OK / 2.0.19.0	OK / 2.0.19.0	OK / 2.0.26.0	OK / 2.0.26.0	OK / 2.0.26.0
Bull/Ingenico www.ingenico.com	STLP2	PCCARD	SCM SCR201 drivers	OK / 3.12.00.00	OK / 3.17.00.01	OK / 3.13.00.00	OK / 3.20.00.01	OK / 3.20.00.01
	STLP3	RS/ PS2	non P&P	OK / 1.0.3+1.00	OK / 1.0.3	OK / 1.0.3	OK / P&P 5.0.2134.1	OK / P&P 5.1.2600.0
Castleswww.casauto.com.tw	EZ100PU	USB	Version 0075	OK / 3.16	OK / 3.16		OK / 3.1.6.0	OK / 3.1.6.0
	EZ220PU	USB	Version 0045	OK / 1.00	OK / 1.00		OK / 1.00	OK / 1.0.0.0
	EZMini	USB	Version 0075	OK / 3.16	OK / 3.16		OK / 3.1.6.0	OK / 3.1.6.0
	Pisces310	USB	Version 0075	OK / 3.16	OK / 3.16		OK / 3.1.6.0	OK / 3.1.6
Compaq www.compaq.com HP www.hp.com	Basic Serial KEYB	RS/ PS2	Gemplus GCR410P drivers	Problems / 2.5.0	Problems / 2.5.5.0	OK / 1.3.3.0	OK / 2.6.1.0	OK / 2.6.1.0

[305] cf. http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/A0D3A8D03E6882C5C22572440052 13EC?opendocument, access on 25.07.2007, 09:15

provider	Model	Type	Driver version	Win 98	Win ME	Win NT 4.0 *	Win 2000 Pro	Win XP Pro
	Easy Access KEYB with Smart Card Reader L2	USB	O2Micro OZ773 drivers	OK / 1.3.5.3	OK / 1.3.5.3	No drivers	OK / 1.3.5.3	OK / 1.3.5.3
Datakey www.datakey.com	KR630	USB	Gemplus GemPC430 drivers	OK / 2.1.0.0	OK / 2.1.0.0	No drivers	OK / 2.1.0.0	OK / 2.1.0.0
Dell www.dell.fi	Dell Latitude D600 Series	Inter-nal	O2Micro OZ711EC1 drivers	Not sup-ported	Not sup-ported	Not sup-ported	OK / 3.0.0.302	OK / 3.0.0.302
	Dell Latitude D620 Series	Inter-nal	O2Micro CCID SC Reader drivers	Not sup-ported	Not sup-ported	Not sup-ported	Not sup-ported	OK / 5.2.3790.2444
	Dell Latitude D820 Series	Inter-nal	O2Micro CCID SC Reader drivers	Not sup-ported	Not sup-ported	Not sup-ported	Not sup-ported	OK / 5.2.3790.2444
Fujitsu-Siemens www.fujitsu-siemens.fi	Lifebook E Series	PCCA RD inter-nal	O2Micro OZ711E1 driv-ers	Being tested	OK / 2.0.5.3	OK / 1.0.0.6	OK / 2.0.5.3	OK / 2.0.5.3
	SCM SCR301	USB	SCM SCR301 drivers	OK / 1.16.00.01	OK / 1.16.00.01	no drivers	OK / 2.10.00.01	OK / 2.10.00.01
Gemplus www.gemplus.com	GCR410P	RS/ PS2		Problems / 2.5.0	Problems / 2.5.5.0	OK / 1.3.3.0	OK / 2.6.1.0	OK / 2.6.1.0
	GemPC410-SL	RS/ PS2		Problems / 2.5.0	Problems / 2.5.5.0	OK / 1.3.3.0	OK / 2.6.1.0	OK / 2.6.1.0
	GemPC410FD	RS/ POW/F		Problems / 2.5.0	Problems / 2.5.5.0	OK / 1.3.3.0	OK / 2.6.1.0	OK / 2.6.1.0
	GemPC410	RS/ PS2		Problems / 2.5.0	Problems / 2.5.5.0	OK / 1.3.3.0	OK / 2.6.1.0	OK / 2.6.1.0
	GemPC430	USB		OK / 2.1.0.0	OK / 2.1.0.0	no drivers	OK / 2.1.0.0	OK / 2.1.0.0
	GemPC USB	USB		OK / 1.0.0.11	OK / 1.0.0.11	no drivers	OK / 1.0.0.11	OK / 1.0.0.11
	GemPC Twin	USB		OK / 1.0.0.11	OK / 1.0.0.11	no drivers	OK / 1.0.0.11	OK / 1.0.0.11
	GemPC Card	PCMC IA		OK / 2.0.0.0	OK / 2.0.0.0	OK / 2.0.0.4	OK / 2.0.0.4	
	GemPC Serial	RS/ PS2		OK / 1.0.5.11	OK / 1.0.5.11		OK / 1.0.5.11	OK / 1.0.5.11
HP Compaq www.hp.fi	HP Compaq nc6220	Inter-nal	TI GemCore drivers	Not sup-ported	Not sup-ported	Not sup-ported	Not sup-ported	OK / 1.0.1.13

provider	Model	Type	Driver version	Win 98	Win ME	Win NT 4.0 *	Win 2000 Pro	Win XP Pro
Omnikey www.omnikey.com, Utimaco Safeware www.utimaco.com	CardMan 2011	RS/ PS2	fw 1.00	OK / 1.0.1.1	OK / 1.0.1.1	OK / 1.0.1.1	OK / 1.0.1.1	OK / 1.0.1.1
	CardMan 3021	USB	fw 2.03	OK / 1.1.1.0	OK / 1.1.1.0		OK / 1.1.1.0	OK / 1.1.1.0
	CardMan 3111	RS/ PS2	fw 2.01	OK / 1.1.0.24	OK / 1.1.0.24	OK / 1.1.0.24	OK / 1.1.0.24	OK / 1.1.0.24
	CardMan 3121	USB	fw 1.01	OK / 1.1.0.24	OK / 1.1.0.24	No drivers	OK / 1.1.0.24	OK / 1.1.0.24
	CardMan 4000	PCCA RD	fw 2.00	OK / 3.5.0.12	OK / 3.5.0.12	OK / 3.5.0.12	OK / 3.5.0.12	OK / 3.5.0.12
	CardMan 4040	PCCA RD	fw 1.00	OK / 1.1.0.38	OK / 1.1.0.38	OK / 1.1.0.38	OK / 1.1.0.38	OK / 1.1.0.38
	CardMan 5010 KEYB	RS/ PS2		OK / 3.4.0.1	OK / 3.4.0.1	OK / 3.4.0.1	OK / 3.4.0.2	OK / 3.4.0.2
	CardMan 5020 KEYB	USB		OK / 3.7.3.12	OK / 3.7.3.12	OK / 3.7.0.1	OK / 3.7.3.12	OK / 3.7.3.12
	CardMan 6020 KEYB	USB/ SIM	fw 2.00	OK / 3.7.3.19	OK / 3.7.3.19	OK / 3.7.0.1	OK / 3.7.3.19	Slow / 3.7.3.19
SCM Microsystems www.scmmicro.com	SCR131 / SCR531	RS/ PS2		OK / 4.04.00.01	OK / 4.04.00.01	OK / 4.09.00.01	OK / 4.04.00.01	OK / 4.04.00.01
	SCR201	PCCA RD	fw 2.41	OK / 3.12.00.00	OK / 3.17.00.01	OK / 3.13.00.00	OK / 3.20.00.01	OK / 3.20.00.01
	SCR241	PCCA RD	fw 2.03, SCM SCR24x drivers	OK / 1.20.00.01	OK / 1.12.00.01	OK / 1.10.00.01	OK / 1.20.00.01	OK / 1.20.00.01
	SCR243	PCCA RD	fw 2.03, SCM SCR24x drivers	OK / 1.20.00.01	OK / 1.20.00.01	OK / 1.10.00.01	OK / 1.20.00.01	OK / 1.20.00.01
	SCR301	USB	fw 3.00	OK / 1.16.00.01	OK / 1.16.00.01	No drivers	OK / 2.10.00.01	OK / 2.10.00.01
	SCR331 / SCR531	USB	fw 4.15 ja 5.18	OK / 4.30.00.01	OK / 4.30.00.01	No drivers	OK / 4.30.00.01	OK / 4.30.00.01
	SCR3310	USB	fw 5.14	OK / 4.24.00.01	OK / 4.24.00.01	No drivers	OK / 4.30.00.01	OK / 4.30.00.01
	SCR3340	EC/54	fw 5.20					OK / 4.31.00.01
	SPR110	RS/ PS2/P		OK / 1.20.007	OK / 1.20.006	OK / 1.20.008	OK / 1.0.2.0	No drivers
	SPR132 / SPR532	RS/ PS2/P	fw 4.12	OK / 4.04.00.01	OK / 4.04.00.01	OK / 4.06.00.01	OK / 4.05.00.01	OK / 4.05.00.01
	SPR132 / SPR532	RS/ PS2/P	fw 4.15	OK / 4.10.00.01	OK / 4.10.00.01	OK / 4.10.00.01	OK / 4.10.00.01	OK / 4.10.00.01
	SPR332 / SPR532	USB/P	fw 4.12	OK / 4.04.00.03	OK / 4.04.00.02	No drivers	OK / 4.04.00.02	OK / 4.04.00.02

provider	Model	Type	Driver version	Win 98	Win ME	Win NT 4.0 *	Win 2000 Pro	Win XP Pro
	SPR332 / SPR532	USB/P	fw 4.15	OK / 4.20.00.01	OK / 4.20.00.01	No drivers	OK / 4.33.00.01	OK / 4.33.00.01
Setec www.setec.fi	SetCAD 203	RS/ PS2	ver 1.4 drivers	Problems / 1.00	Problems / 1.0.0.0	OK / 4.00	OK / 4.0.1381.1	Problems / 4.0.1381.1
Todos Data System www.todos.se	Argos Mini Serial	RS/U		OK / 1.41	OK / 1.41	OK / 1.41	OK / 1.0.0.1	OK / 1.0.0.1
	Argos Mini	USB		OK / 2.4.2	OK / 2.4.2.0	No drivers	OK / 2.4.2.0	OK / 2.4.2.0
	Argos Mini II	USB		OK / 2.5.2.9	OK / 2.5.2.9	No drivers	OK / 2.5.2.9	OK / 2.5.2.9
Towitoko www.towitoko.de	Chipdrive micro 100	RS/ PS2		OK / 3.06.00.01	OK / 3.06.00.01	OK / 2.14.41	OK / 3.06.00.01	OK / 3.06.00.01

Certificate requirements

When using Population register Centre's certificates, a software is required, as well as a card and card and a card reader.[306]

To use the FINEID card, specific middleware applications have been developed by different companies, like Setec/Gemalto, Fujitsu Services Finland, Nexus/ID2 or SSH Communications. Also an OpenSource project supports the FINEID.
The middleware applications can also be used with other types of smartcards beside the FINEID card.
One example of a middleware application is the SetWeb middleware that was developed by Setec/ Gemalto. It is free available for all card holders and supplies the key interface for many eGovernment services.[307]

The Population Register Centre issues e-mail Certificates. This e-mail certificates are file-based, so no card reader or further software is needed and works for the most e-mail software that supports S/MIME messages.[308]

Application programming interface for online-verification

If an ID card with certification is lost it has to be reported to the revocation list that includes all cancelled certificates. This revocation list is published by the Population Register Centre in connection with a directory service of certificates.[309]

---

[306] cf. Correspondence with Johannes Brunner, commercial attaché for Finland, Estonia. Latvia and Lithuania, Federal Economic Chamber, foreign trade office, Helsinki

[307] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[308] cf. http://www.fineid.fi/vrk/fineid/home.nsf/pages/C3B39DB2DB61D6B7C2257054002DB718, access on 25.07.2007, 09:17

[309] cf. http://www.vaestorekisterikeskus.fi/vrk/fineid/home.nsf/pages/11536F2A8FC6C794C225705 4002DEC65, access on 24.07.2007, 09:48

At the moment, an Online Certificate Status Protocol service is not provided by PRC.[310]

2.8.4 Summary

Table 30 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 30: Summary and rating, Finland, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2003. 2003, agreement with Estonia for harmonisation of application, document format and exchange,	A
technical standard	eGov, eHealth, eDeclaration, eBanking advanced and qualified electronic signatures qualified Certificate on ID card, mobile SIM card, possibility to combine it with health insurance card, software certificates (s/MIME), server certificates only 1 CSP issuing qualified certificates FINEID card, mobile SIM huge range of card readers recommended CRL	A
distribution	Use of Q eS in eGov applications is not wide spread as the use of FINEID is only optional eDeclaration: 120.000 companies registered, is Finland‘s most used eGov portal, around 0,2% of the users access via FINEID In July 2007, already 153.600 Citizen Certificates have been issued, electronic signature is not often used for eGovernment services.	A

[310] cf. Correspondence with Johannes Brunner, commercial attaché for Finland, Estonia. Latvia and Lithuania, Federal Economic Chamber, foreign trade office, Helsinki

2.9 France

Figure 33: Fact-sheet: France, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 33 some basic demographic and geographic data of the country is presented.

2.9.1 Institutional frame

Legislation

France has adopted a range of regulations for electronic signatures:

- Act on „Adaption of the Law of Evidence on Information Technology and Relevant to e-signatures“
- Decree on „Implementing the new Modification of the Civil Code and relating to e-signatures
- Decree on the „Evaluation and Certification of the Security ensured by e-signatures Products and Systems“
- Decree on „the Qualification of CSPs and the Accreditation of the Evaluation Bodies“
- March 2000: Law on electronic Signature (see Appendix - France: Law on electronic Signature, only available in French)

The Act assimilates electronic signature to handwritten signature if certain requirements are fulfilled, like identification or the link between signature and content. The electronic signature is held reliable when the signature has been created, the identity of the signatory assured and the integrity guaranteed.[311]

[311] Study of the Donau Universität Krems, Master-Studie, Frankreich

The Law does not set out cases in which electronic signatures can not be used. Furthermore, it makes no difference between the legal value between an electronic signature created by a natural person and a legal person.[312]

An electronic signature is regarded as reliable if it is created with a secured signature creation device and if it is based on a qualified certificate.[313]

•recognition of foreign certificates:[314]
In March 1998, an agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:
Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of Online Services

•eGovernment:[315]
France is anxious to offer eGovernment services and developed a range of activities since the mid 90‘ to prepare the country for an information society. This haas been realised partly by the Administration Electronique project (ADELE project). The results of all efforts can be seen on the central portal https://www.administration24h24.gouv.fr/. The France government offers a range of electronic services to citizens, businesses and local communities. The portal is modified and updated permanently. On the 1st of Mach 2007, the portal offered 40 online services for citizens, like family allowances, student‘s scholarships, home address changes, exchange of health insurance forms.
The objective for 2008 is to provide every user personal space at www.mon-servicepublic.fr and shall enable users to store personal documents online (like the birth certificate or the tax declarations).

---

[312] cf. Study of the Donau Universität Krems, Master-Studie, Frankreich

[313] cf. Menais, Alexandre, Electronic Signatures in France, July 2002, http://www.juriscom.net/en/pro/1/ec20020730.htm, access on 12.11.2007, 13:46

[314] cf. Study of the Donau Universität Krems, Master-Studie, Austria

[315] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•eProcurement:[316]

Since 2006, public procurement procedures can be effected in France. The French government offers enterprises the possibility to transmit online offers via an interactive portal „Salle des Marchés“ (http://www.achatpublic.com). The electronic transmissions occur via the interactive portal and require a signature certificate that is compliant with PRISv1 technical specifications. The signature must be advanced and on basis of a qualified certificate. The certificate can be created by a secure USB key or a chip card, that are issued by a qualified certificate service provider.

The portal offers a lot of information how to process an electronic transmission and where to obtain a necessary certificate. Companies that want to apply for such a certificate must be established in France.

There are no statistics on the use of electronic signature but in 2006, applicants have loaded about 70.000 calls for tender down. The main page of the portal is shown in figure 34.

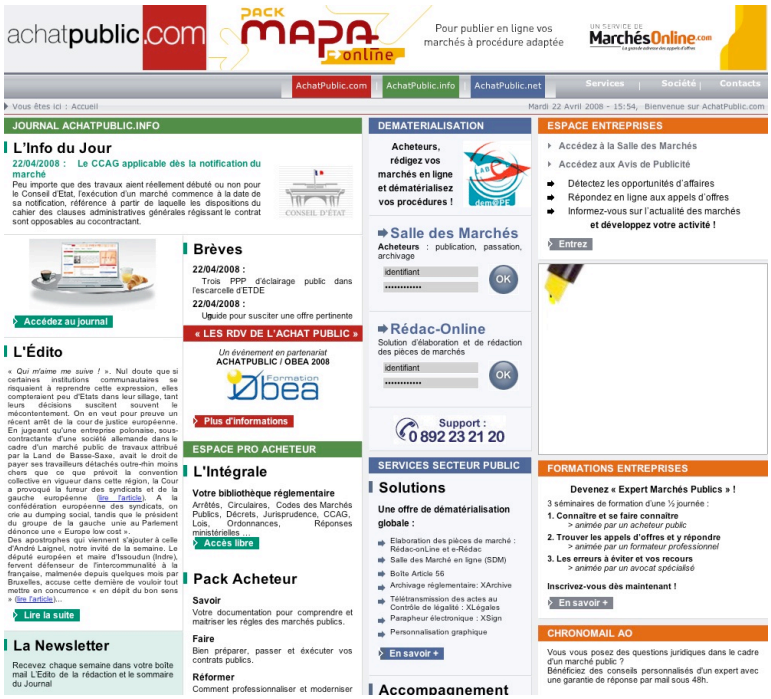


Figure 34: Online portal „Salle des Marchés“ on achatpublic.com, source: http://www.achatpublic.com,access on 12.11.2007, 17:01

Beside achatpublic.com, the Ministry of Defense developed a separate e-procurement portal, accessible at www.marches.achats.defense.gouv.fr. Transactions on this portal also require advanced electronic signatures based on qualified certificates.[317]

[316] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[317] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•Social security:[318]

The French Social Security system offers a secure platform Net-entreprises.fr to allow companies and representatives to declare and pay Social Security contributions online.

The platform can be accessed by using either passwords or digital certificates. The certification service providers that are recognized by the system are listed at http://www.net-entreprises.fr/html/certificat.htm.

In the period between January 2006 and April 2007, about 2,25 million declarations have been registered. No statistics have been available on the use of electronic signature.

Besides Net-entreprises.fr, other portals also offer social security information and services, but typically use password for authentication instead of electronic signatures.

•eTax:[319]

In France, the central portal for online tax declarations is www.impots.gouv.fr, offering services for enterprises and individuals. But the applications for online tax declarations for individuals do not use electronic signatures, but only the unique fiscal number in combination with a password that can be obtained at the administration.

The catalogue for enterprises is much larger. The system for enterprises (EDI - Echange de Formulaires Informatisés) requires secure electronic signatures based on digital certificates that is issued by a recognized certification service provider.

The application for VAT declaration is called TéléTVA. This system currently relies only on a simple signature process, using only soft certificates.

Since 2006 all enterprises that have a turnover over 1.5 million euros must declare and pay their VAT online. Monthly about 250.000 enterprises uses electronic signature for this service.

•Tele-c@rtegrise - eService for the automobile industry:[320]

In 2003, the Ministry of Finance presented a new eService for the automobile industry. This services is called Télé-c@rtegrise and enables professionals different online services and operations concerning car registration, like purchase or sale declarations, demands for registration or (since July 2006) declaration for destruction of vehicles that are already out of order. The professionals can also transmit data to the „national vehicles registration file“ of the Minister de l‘Interieur.

To use Télé-c@rtegrise an electronic certificate is required for authentication. The certificate can either be on a chip card or on an USB key.

Also this system distinguishes between enterprises and individuals. Enterprises can log in via a secure electronic signature based on a digital certificate, issued by a recognized certification service provider.

For individuals, the Ministry of Interior is in contract with Certinomis. When logging in, Certinomis[321] installs a Certinomis certificate on the user‘s computer with that the user can be authenticated.

---

[318] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[319] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[320] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[321] see http://www.certinomis.com

Types of electronic signature

The French law recognizes three types of electronic signature:[322]

1. simple digital signature: consists in a reliable identification process that guarantees its link with the document to which it is attached.
2. secured digital signature: is a digital signature that meet a number of requirements.
3. digital signature benefiting from a presumption of reliability: is a secure digital signature that meets some extra requirements. In case of dispute on the value of the established signature, the burden of proof of non-validity lies on the person disputing this validity and not on the signer.

Unlike in the EU Directive, the french law doesn't use the term „advanced electronic signature" but „secure", which means that the signature is linked to the signatory and linked to the data of the document.

The Platform achatpublic.com requires advanced electronic signatures based on qualified certificates to submit electronic bids in the context of public procurement.[323]

2.9.2 Application requirements

Types of certificates

The public procurement platform for achatpublic.com requires advanced electronic signature based on qualified certificates. The certificate can be created by a secured USB key or be on a chip card, issued by a qualified certification service provider.

Electronic tax declarations can be submitted by the central portal www.impots.gouv.fr. The system requires a secure electronic signatures based on digital certificates (for enterprises).

The application for VAT declaration is called TéléTVA. TéléTVA currently uses a simple signature process, using soft certificates.

The eServices offered for the automobile industry (Télé-c@rtegrise) requires an electronic certificate to authenticate the enterprise. The certificate must be on a chip card or an USB key. [324]

Certification Service Providers

Currently the qualified certificate service provider are the following (table 31):[325]

---

[322] cf. Study of the Donau Universität Krems, Master-Studie, Frankreich

[323] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[324] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[325] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Table 31: Qualified Certification Service Provider France, source: own illustration

Certification Service Provider		Web site/adress
Atos Origin		http://www.fr.atosorigin.com
Azzarius		AZZARIUS Locasystem Media Centre Sud Affaires de BELFORT 6 Rue du Rhône Centre Sud Affaires, Bâtiment A 90000 BELFORT Tel : +33 (0) 9 51 46 90 90 Fax : +33 (0) 1 39 22 40 32 Mail : contact@azzarius.com
BNP Paribas		www.bnpparibas.com
Certeurope		34-36, rue de la Folie Régnault 75011 Paris Tél : 01 45 26 72 00 Fax : 01 45 26 72 01 http://www.certeurope.fr/
Certinomis		Service commercial 20-22 rue Louis Armand 75015 PARIS T 0 826 826 62 http://www.certinomis.com
chambersign		Service commercial Chambre de Commerce et d'Industrie de Lyon Place de la Bourse 69002 Lyon Téléphone 08 92 23 02 52 support@chambersign.tm.fr www.chambersign.tm.fr
Click and Trust Groupe Banque Populaire		Click & Trust SA - 18, quai de la Rapée - 75012 Paris téléphone : 0892 68 14 18 fax : +33 (0)1 40 04 95 22 contact-commercial@click-and-trust.com
Credit Agricole		http://www.credit-agricole.fr/
Credit Lyonnais		https://www.lcl.fr/
Greffe TC-Paris		Greffe du Tribunal de commerce de Paris 1, quai de la Corse 75181 PARIS Cedex 0 http://www.greffe-tc-paris.fr/
HSBC France		http://www.hsbc.fr
Infogreffe		Infogreffe - Centre Daumesnil - 4 place Félix Eboué 75583 Paris cedex 12 T 0891 01 11 11 http://www.infogreffe.fr

Certification Service Provider		Web site/adress
Natexis Banques Populaires	NATIXIS	http://www.NATIXIS.COM
SG Trust Services	SG TRUST SERVICES	SG Trust Services – Customer Service CS 3313 41033 BLOIS CEDEX, FRANCE Phone : +33(0) 2 54 44 71 07 Fax : +33(0) 2 54 44 43 57 E-mail: hotline@sgtrustservices.com http://www.sgtrustservices.com/

•Other signature service providers:

➡short description: Keynectis:
1998 the enterprise Certplus was founded as national trustcenter in France. Since 2004, the enterprise is named Keynectis.[326]
Keynectis offers among other products and services „signature to pdf“ solutions and SSL Certificates.[327]

➡short description: Thawte
The world wide operating enterprise Thawte is also acting on local market.
Thawte is owned by VeriSign but operates as distinct brand within the stable of VeriSign.
VeriSign offers among other products SSL Certificates.[328]

Table 32 sums all other certification service providers in France:

Table 32: Other Certification Service Provider in France, source: own illustration

Certification Service Provider		Issues Certificates
Keynetics	KEYNECTIS	SSL
VeriSign	VeriSign	SSL

Inspecting authorities

The authority for supervision in France is the Direction centrale de la securite des systemes d'information (DCSSI).[329]

[326] cf. http://www.certplus.com/, access on 13.11.2007, 11:37

[327] cf. http://www.keynectis.com/en/index.html, access on 14.11.2007, 19:37

[328] cf. http://www.verisign.fr/ssl/index.html, access on 14.11.2007, 19:47

[329] cf. http://www.ssi.gouv.fr/fr/index.html, access on 14.11.2007, 19:56

2.9.3 Technical preconditions

Signature Software

The French Telecom[330] provides accredited signature products named Applatoo. It is a platform that enables secure electronic exchanges in the eBusiness area with legal force. On the platform, the user can work with digital certificates and time-stamps. Authentication and encryption is enabled by the platform and certification revocation lists can be checked online. Applatoo is compatible with all client environments (Windows 98, Windows 2000, Windows XP, Windows 2003, Mac 8.,Mac 9., Mac X., Linux) and works in the most web browsers (Explorer, Modzila, Netscape, Safari).[331]

The project FAST provides a solution as well, called „Fast Signature“, that is available for the area of digital signature and eGovernment.

The company Dictao also issues signature solutions, like the software AdSigner (figure 35). AdSigner was the first software for electronic signature creation that is certified under Common Criteria at EAL3+ level and qualified.
This software was used by over 7 million citizens in 2007 to sign online tax declarations.

Figure 35: AdSigner signature software solution, source: http://www.dictao.com/, access on 14.11.2007, 21:!3

Types of secure signature-creation device

•eID Card:
In 2003, first plans for an electronic identity card CNIE (Carte Nationale d‘Identité Electronique) were announced by the French Ministry of the Interior. CINE is part of the Identification Nationale Electronique Securisee programme that aims to

- simplify and harmonize procedures for requesting national ID cards and passports and secure that procedures
- improve applications to manage documents
- deliver high secure documents

[330] see www.francetelecom.fr

[331] cf. http://www.ilex.fr/en/produits/applatoo-presentation.htm, access on 14.11.2007, 19:51

- offer citizens the possibility to prove their identity in the Internet and electronically sign documents
- further the development of e-administration.

The roll out of CINE was planned for 2006 but was postponed.[332]

The next generation is the Vitale card (figure 36) for the health sector. The card complies with the IAS standards (Identification, Authentication, Signature) and meets new requirements of the welfare and health field.

Figure 36: Vitale Card, source: http://www.modernisation.gouv.fr/uploads/RTEmagicC_SesamVitale2_06.jpg.jpg, access on 14.11.2007, 19:48

Currently, the Vitale card links over 223.000 health care professionals to the French Health Insurance System. This card is the most used, the infrastructure incorporates components like

- 48 million smartcards,
- 210.000 smart card readers,
- 230 health software applications,
- 25 servers
- 23.000 terminals for updating the card.[333]

Since 2006, the French government offers enterprises the possibility through the portal „Salle des Marches“ to transmit online offers. The bids must be provided by an advanced electronic signature based on a qualified certificate. The certificate can be on a secured USB key or a chip card, issued by a qualified certificate service provider.[334]

Card readers

n.a.

[332] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, source: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[333] cf. GIE sesam viatale, the SESAM-Vitale program, http://www.sesam-vitale.fr/programme/programme_eng.asp, access on 14.11.2007, 19:46

[334] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Certificate requirements

n.a.

Application programming interface for online-verification

The electronic tax declaration system uses CRL and OSCP validation protocol for validate the electronic certificates.[335]

2.9.4 Summary

Table 33 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 33: Summary and rating, France, source: own illustration

categories		rating
legal framework	There are a lot of Acts and decrees that regulate electronic signatures, producs and systems. In March 2000, the Law on electronic signatures was implemented.	A
technical standard	eGov, eProcurement, eTax, other eServices, all types of electronic signatures, basic and qualified certificates eID card, CardVitale huge range of certification service provider, issuing qualified certificates	A
distribution	Monthly about 250.000 companies use electronic siganture to submit their Tax declarations electronically to the Tax Administration. Vitale card links over 223.000 health care professionals to Health insurance system (48 million smartcards, 210.000 card readers, 230 health software application) CRL, OSP	A

[335] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

2.10 Germany

Figure 37: Fact-sheet: Germany, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 37 some basic demographic and geographic data of the country is presented.

2.10.1 Institutional frame

Legislation

Germany was one of the first countries that adopted a Signature Law in 1997[336]. On 22 July 1997, the German Parliament approved the „Digital Signature Law" that creates general conditions under which a digital signature is deemed secure and reliably (see Appendix - Germany: Digital Signature Act, SigG). The transformation on technical is furthermore regulated by the corresponding signature ordinance (Signaturverordnung, SigV, see Appendix - Germany: Digital Signature Ordinance, SigV).[337] As there is no official version in English of SigG and SigV, both are offered in German.

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Germany: National Regulations Details.[338]

[336] cf. Politik-digital.de, Mit digitaler Signatur und Internet-Payment ins virtuelle Rathaus, Expertenchat zum Thema in Kooperation mit NADIV, 25.April 2001, http://www.politik-digital.de/salon/transcripte/sklein.shtml, access on 14.11.2007, 18:13

[337] cf. Correspondence with Stephan Scholz, ederal Office for Information Security (BSI), Service Center, Bonn

[338] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•recognition of foreign certificates:
According to §23 paragraph 1 SigG, certification service provider from other European countries are equal to domestic providers if they fulfill the EU directive.

In March 1998, the agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:
Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.[339]

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:[340]

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of Online Services

•eGovernment
In the year 2000, the topic of eGovernment was announced to be a central issue and the initiative BundOnline 2005 was started (logo can be seen in figure 38).[341] BundOnline effectuated to offer about 440 informations about the online services of government, businesses and authorities online until 2005. Therewith, BundOnline is classified as one of the momentously eGovernment initiatives in Europe.[342]

Figure 38: BLogo BundOnline, source: http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/Initiativen/Bol/bol.html__nnn=true, access on 14.11.2007, 18:34

[339] cf. Study of the Donau Universität Krems, Master-Studie, Austria

[340] cf. Study of the Donau Universität Krems, Master-Studie, Austria

[341] for more information see http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/Initiativen/Bol/bol.html__nnn=true

[342] cf. Bundesministerium des Inneren, E-Government, http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/egov__inhalt.html, access on 02Nov08

Based on the gained experiences from the initiative BundOnline, the government enacted the program E-Government 2.0 on the 13th September 2006 (logo can bee seen in figure 39). The Government identified 4 spheres of activity that shall be developed and extended in the next years until 2010. Thus, the modernization process in the administration will be brought forward by e-Government. The 4 spheres of activity concern:

- portfolio: qualitative and quantitative development of eGovernment proposition
- process chain: electronic co-operation between economy and administration by combined process chains,
- identification: introduction of an electronic identity card and formulation of e-identity concepts
- communication: secure communication infrastructure for citizens, businesses and administration.

Figure 39: Logo e-Gocernment 2.0, source http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/Initiativen/EGov2/EGov2.html__nnn=truem access on 14.11.2007, 18:27

Internet should be so the preferential communication and distribution channel. Secure transaction will be easier within e-Government and e-business with electronic identity cards and citizens preserve certificated citizen portals where thy can communicate in an easy secure and antonym way. On the 20 February 2007, the realization plan was concluded and 25 projects have been announced, with that the e-Government will be developed and enlarged service oriented.[343]

Lately, the virtual mail-administration center of Federation (Virtuelle Poststelle VPS), was evaluated and certified. This VPS is an eGovernment communications gateway that enables legally binding electronic signatures.

•eInvoice

Annually, German businesses issue over 6 million of invoices. The trend veers toward to electronic invoics.[344] When issuing electronic invoices, businesses have to mark that the law demands qualified electronic signatures. Without such a signature, the invoice recipient cannot claim for an input tax deduction.[345]

---

[343] cf. Federal Ministry of the Interior, Federal Government Co-ordination and Advisory Agency for IT in the Federal Administration, E-Government 2.0 - Programm des Bundes, http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/Initiativen/EGov2/EGov2.html__nnn=true, access on 6.11.2007, 17:56

[344] cf. Arbeitsgemeinschaft für wirtschaftliche Verwaltung, Der elektronische Rechnungsaustausch, http://www.awv-net.de/cms/font_content.php?idcat=23&prod_id=68, access on 09.08.2007, 09:24

[345] cf. ECIN, Digitale Rechnungen: aber sicher!, press release, 10.5.2005, http://www.ecin.de/news/2006/05/10/09472/index.html, access on 14.11.2007, 19:05

The AWV-Consortium for commercial administration (AWV-Arbeitsgemeinschaft für wirtschaftliche Verwaltung[346]) has published a brochure „Der elektronische Rechungsaustausch - Ein Leitfaden für Unternehmen zur Einführung elektronischer Rechnungen“. This brochure addresses to small and medium-sized businesses to answer questions concerning electronic issuing of invoices, both technical, legal and economical problems.[347]

To sign invoices electronically, high investments in hard- and software must be made, thus mass signatures were only rentable for large firms. For this reason, a system was developed to support small and medium sized enterprises: rechnung.de. The partner for the implementation of this system was D-Trust, that cared for the necessary security. The System transmitts the documents to a signature card at D-Trust, where it gets a signature stamp and a qualified electronic signature. Thereafter, the eMails are submitted automatically to the invoice addressee.[348] The main page of rechnung.de is shown in figure 40.

Figure 40: rechnung.de, source: http://www.rechnung.de/, access on 14.11.2007, 19:06

•eTaxing

Within the ELSTER project, a secure platform has been developed for the online Portal ElsterOnline, enabling to submit the tax return electronically with the use of electronic signature.

[346] for more information see http://www.awv-net.de

[347] cf. Correspondence with Stephan Scholz, ederal Office for Information Security (BSI), Service Center, Bonn

[348] cf. ECIN, Digitale Rechnungen: aber sicher!, press release, 10.5.2005, http://www.ecin.de/news/2006/05/10/09472/index.html, access on 14.11.2007, 19:06

•other eServices:
All operational and planned eGovernment applications are summed up in the Appendix - Germany: Operational and planned applications. [349]

•High security cachets:
The regulation authority for Telecommunication and Post (Reg TP) deals two new seals of approvals, one for TrustCenters, one for products for qualified electronic signatures (figure 41).
The cachet with addition „accredited“ is issued for Trust Centers and guarantees that the center is accredited and fulfills high technical and administrative safety requirements of SigG.
The other cachet without addition is issued for signature products that meet the high safety requirements of SigG, for example card readers, chip cards or application software.[350]

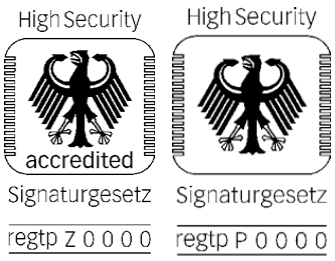


Figure 41: cachets for TrustCenters and electronic signature products, source: Federal Network Agency, Gütezeichen Elektronische Signatur, press release, 15.3.2002, source: http://www.bundesnetzagentur.de/enid/cdaaa2fe5fc787790561773fd4d1f4ce,0/Archiv_Pressemitteilungen/PM_2__2_-_Jan_-Juni_ax.html#563, access on 14.11.2007, 19:14

Types of electronic signature

The „Digital Signature Law“ defines digital signature as „a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority.“[351]

The Law SigG defines 3 different types of electronic signature:[352]

- basic electronic signature (§2 No 1 SigG): to identify the originator of an electronic message, for example by saving a scanned signature, no requirements are defined, only little authenticity

[349] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[350] cf. Federal Network Agency, Gütezeichen Elektronische Signatur, press release, 15.3.2002, http://www.bundesnetzagentur.de/enid/cdaaa2fe5fc787790561773fd4d1f4ce,0/Archiv_Pressemitteilungen/PM_2__2_-_Jan_-Juni_ax.html#563, access on 03NOV07

[351] cf. German Digital Signature Law, see Appendix Germany

[352] cf. Federal Office for Information Security, BSI-Kurzinformation, Elektronische Signatur, http://www.bsi.bund.de/literat/faltbl/F10ElektronischeSignatur.htm, access on 14.11.2007, 19:16

- advanced electronic signature (§2 No 2 SigG): make manipulation of data cognizable, identify a natural person, higher authenticity depending on used signature method and software- and hardware components
- qualified electronic signature (§2 No 3 SigG): highest security level, based on qualified certificate by certification service provider (trust center), equal treatment with handwritten signature

The Federal office for Information Security (Bundesamt für Sicherheit in der Informatinstechnologie, BSI) offers electronic signature for the following application area:

- E-Mail,
- word processing,
- spreadsheet analysis.[353]

T7 e.V. issues a public and free online information desk, where the user can search for points of acceptance for qualified electronic signatures. At www.signaurauskunft.de, private user, businesses, institutions and agencies can find acceptance points and applications for their signatures. The information include names and addresses of responsible centers, descriptions and continuative links. Actually about 842 points of acceptance and applications are recorded.[354]

➡Short descrition T7 e.V.
The consortium was founded in 1999 and is a registered association and professional institution since January 2005. The aim is to build an operation platform and representation of interests for businesses, that supply services and products for electronic signature to create secure standards.
T7 e.V. is a consortium of Trust Center and Certification Service Provider. Members are supplier of chip cards and certificates that are precondition for qualified electronic signature according to SigG. T7-members are DATEV eG, D-Trust GmbH, Deutsche Post Com GmbH, Deutscher Sparkassenverlag, TC Trustcenter GmbH and the Deutsche Telekom AG. [355]

2.10.2 Application requirements

Types of certificates

The qualified electronic signature is based on a qualified certificate, issued by a certification service provider.[356]

---

[353] cf. Federal Office for Information Security, FAQs on electronic signature, http://www.bsi.bund.de/esig/faq.htm, access on 14.11.2007, 19:16

[354] cf. t7 e-V., Verzeichnis der akzeptanzstellen für qualifizierte elecktronische Signaturen, press release, 28.march 2006, www.signaturauskunft.de, access on 14.11.2007, 19:24

[355] cf. http://www.t7ev.org/index.php?id=394, access on 14.11.2007, 19:39

[356] cf. Federal Office for Information Security, BSI-Kurzinformation, Elektronische Signatur, http://www.bsi.bund.de/literat/faltbl/F10ElektronischeSignatur.htm, access on 14.11.2007, 19:16

About 25.000 qualified certificates stored on secure signature creation devices, have been issues in Germany.[357]

Certification Service Providers[358]

•accredited certification service provider, issuing qualified certificates and qualified timestamps:

➡Short description: Deutsche Telekom Telesec[359]
The Deutsche Telekom Telesec was the first Trust-Center in Germany accredited by the Signature Law and is accredited since 22.12.1998.

The *Bundesnotarkammer* is accredited since 14.12.2000.

The *DATEV eG Cerfitication Authority* is accredited since 09.03.2001.

The *D-Trust GmbH* is accreditied since 08.03.2002.

The *Deutsche Post Com GmbH* is accredited since 17.09.2004.

➡Short description: TrustCenter[360]:
TrustCenter is one of the leading providers of certificates and security solutions in the area of identity verification. the product portfolio reaches from web-secure services to the protection of eCommerce transactions up to complex PKI solutions. The TrustCenter is accredited since 24.05.2006.

•Accredited certification service provider issuing qualified certificates:

The *DGN Deutsches Gesundheitsnetz Service GmbH* is accredited since 09.08.2007

•Accredited certification service provider issuing qualified timestamps:

The *AuthentiDate International AG* is accredited since 09.11.2001.

•Other certification service provider:

---

[357] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[358] cf. Federal Network Agency, Certification Service Provider, http://www.bundesnetzagentur.de/enid/Elektronische_Signatur/Zertifizierungsdienstanbieter_ph.html, access on 14.11.2007, 19:09

[359] cf. Politik-digital.de, Mit digitaler Signatur und Internet-Payment ins virtuelle Rathaus, Expertenchat zum Thema in Kooperation mit NADIV, 25.April 2001, http://www.politik-digital.de/salon/transcripte/sklein.shtml, access on 13.11.2007, 11:36

[360] cf. http://www.trustcenter.de, access on 06.11.2007, 16:43

Secunet

Secunet is a trust center that is conform with the German Electronic Signature Act.

TeleTrusT

Table 34 lists up all certification service providers in Germany:

Table 34: Certification Services Providers in Germany, source: own illustration

Certification Service Provider		Issued Certificates
TeleSec		qualified certificates qualified timestamps
Bundesnotarkammer		qualified certificates qualified timestamps
DATEV eG Certification Authority		qualified certificates qualified timestamps
D-Trust GmbH		qualified certificates qualified timestamps
Deutsche Post Com GmbH		qualified certificates qualified timestamps
TC TrustCenter GmbH		qualified certificates qualified timestamps
DGN Deutsches Gesundheitsnetz Service GmbH		qualified certificates
AuthentiDate International AG		qualified timestamps
Secunet		n.a.
TeleTrust		n.a.

Inspecting authorities

The Federal Network Agency (Bundesnetzagentur für Elektrizität, Gas, Telkommunikation, Post und Eisenbahn[361]) is the responsible authority according to §3 SigG.

2.10.3 Technical preconditions

Signature software

n.a.

[361] for more information see http://www.bundesnetzagentur.de/enid/Bundesnetzagentur/Die_Bundesnetzagentur_2u.html

Types of secure signature-creation device

The Federal Network Agency recommends the following products for qualified electronic signatures (table 35):[362]

Table 35: Supported Smart Cards by Federal Network Agency, source: http://www.netzagentur.de/enid/409c64ff38ce239a1936c1ff8c37a425,0/Produkte/Sichere_Signaturerstellungseinheiten_vt.html, access on 03Nov08

Type	model
Telesec	PKS-Card Version 1.0
	PKS-Card Version 2.0
	PKS-Card, E4KeyCard, E4KeyCard, E4NetKeyCard, Version 3.0
Signtrust	SEA-Card Version 1.0
	SEA-Card Version 2.0
DATEV	e:secure-Card Version 1.0, new versions e:secure-Card Version 1.10 an e:secure-Card Version 1.20
STARCOS	STARCOS SPK2.3 with digital signature application StarCert (limited signature generation configuration)
	STARCOS SPK2.3 with digital signature application StarCert (unlimited signature generation configuration)
D-TRUST	D-Trust-Card Version 1.0 new versions D-Trust Card Version 1.1 and D-Trust Card_MS Version 1.0
signature creation units	Chipcard with processor, SLE66CX320P, operating system CardOS/M4.01 with application for digital signature, conform with SigG, SigV and DIN V 66291-1
	Chip card with processor SLE66CX322P, operating system CardOS/M4.01A wit application for digital signature
	MICARDO Elliptic Version 2.3 136/32 R1.0 Signature card Version 1.0
	chip card with processor SLE66CX320P, operating system SetCOS 4.4.1 with signature application SetEID v1.0
	ZKA Banking Signature Card, Version 6.2 NP, Type 3, Giesecke & Devrient GmbH
	ZKA-Signature card, Version 5.02, Gemplus-mids GmbH
	Chip card with processor SLE66CX322P, operating system CardOS V4.3B with application for digital signature
	STARCOS 3.1 ECC with Electronic Signature Application V4.0, Version 1.0
	RegTP-Card, Version 3.0, Regulation Authority for Telekommunication and Post
	ZKA Banking Signature Card, Version 6.2b NP and 6.2f NP, Type 3, Giesecke & Devrient GmbH
	ZKA Banking Signature Card, Version 6.31 NP, Type 3, Giesecke & Devrient GmbH
	ZKA Banking Signature Card, Version 6.3 NP, Type 3, Giesecke & Devrient GmbH
	ZKA Banking Signature Card, Version 6.32 NP, Type 3, Giesecke & Devrient GmbH
	ZKA Banking Signature Card, Version 6.4 NP, Type 3, Giesecke & Devrient GmbH
	STARCOS 3.0 with Electronic Signature Application V3.0, Giesecke & Devrient GmbH
	ZKA signature card, Version 5.10, Gemplus GmbH
	ZKA Banking Signature Card, Version 6.6, Giesecke & Devrient GmbH
	ZKA Banking Signature Card, Version 6.51, Giesecke & Devrient GmbH
	ZKA SECCOS Sig v1.5.2
	TCOS 3.0 Signature Card, Version 1.0 with Phillips chip P5CT072V0Q / P5CD036V0Q

[362] cf. Federal Network Agency, Products for qualified electronic signature, netzagentur.de/enid/409c64ff38ce239a1936c1ff8c37a425,0/Produkte/Sichere_Signaturerstellungseinheiten_vt.html, access on 14.11.2007, 19:17

Secunet provided the German pension insurance association in Berlin with employee chip cards, which were successfully launched in 2005. The chip cards enable generation qualified electronic signatures. Employees can authenticate in the network, sign documents electronically and so proceed transactions completely electronically. Furthermore, the cards can be used for access control, PC access and working time processing.[363]

➡short description: secunet
Secunet supplies applications for the use of certificates and central infrastructure for trust centers.[364]

Card readers

The Federal Network Agency recommends the following card readers:[365]

- Chipkartenlesegeräte CardMan®:
  CardMan® , CardMan® Compact, CardMan® Keyboard, CardMan® Mobile, in Verbindung mit der Software CardMan® Software Development Kit, Version 2.2 und einer Prüfsoftware
- Chipkartenlesegerät HML 5010 oder 5020 oder 5021 oder 5022, Version 1.0
- Chipkartenlesegerät cyberJack, Version 3.0
- Siemens Sign@tor Version 1.0
- PC-Tastaturen mit Chipkartenterminal G83-6700LPZxx/00, G83-6700LQZxx/00, G81-7015LQZxx/00, G81-8015LQZxx/00, G81-12000LTZxx/00, G81- 12000LVZxx/00 der Cherry GmbH KOBIL Chipkartenterminals KAAN Professional und B1 Professional HW-Version KCT100, FW-Version 2.08 GK 1.04
- Signaturanwendungskomponente "Sign@tor Version 2.0"
- CyberJack e-com, Version 2.0
- CyberJack pinpad, Version 2.0
- KOBIL Klasse 2 Chipkartenterminals KAAN Standard Plus, FW-Version 02121852 und SecOVID Reader Plus, FW-Version 02121812
- Chipkartenleser SPR132, SPR332, SPR532, Firmware Version 4.15
- Chipkartenleser, cyberJack pinpad, Version 3.0
- Chipkartenterminal der Familie SmartBoard xx44 Firmware-Version 1.04
- Chipkartenterminalfamilie KBPC CX / CX Top: S26381-K329-V1xx HOS:02, S26381- K329-V4xx HOS:01, 26381-K339-V1xx HOS:01, Firmware-Version 1.04 der Fujitsu Siemens Computers GmbH
- Signaturanwendungskomponente Chipkartenterminal der Familie CardMan Trust CM3621 / CM3821, Firmware-Version 6.00
- Chipkartenterminal der Familie SmartTerminal ST-2xxx, Firmware Version 5.08
- Chipkartenleser SPR532 Firmware Version 5.10

---

[363] cf. Secunet Security Networks AG, Public key infrastructures and certificate-based applications, www.secunet.com/fileadmin/ Downloads/ Englisch/Factsheets/Public-key_infrastructure_e.pdf, access on 6.11.2007, 19:52

[364] cf. Correspondence with Thomas Stürznickel, head of Business Security, Secunet Security Networks AG, Germany

[365] cf. Federal Network Agency, Products for qualified electronic signature, chip card readers, http://www.bundesnetzagentur.de/ enid/409c64ff38ce239a1936c1ff8c37a425,0/Produkte/Chipkartenleser_w0.html, access on 14.11.2007, 19:18

- Chipkartenterminal KAAN Advanced, Firmware Version 1.02, Hardware Version K104R3
- Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06

Certificate Requirements

To create electronic signatures, some signature application components are required. The Federal Network agency recommends the following components on their homepage:[366]

•Programs:

- Signtrust Anwenderkomponente eTrust Mail Version 1.01 für Microsoft® Outlook®
- Signtrust Anwenderkomponente eTrust Mail für Microsoft® Outlook® Version 1.11
- Anwenderkomponente GERVA Version 1.0
- Signtrust Anwenderkomponente eTrust Mail für Lotus Notes ® R5 Version 1.01.
- Anwenderkomponente GERVA Version 1.11
- Anwenderkomponente SignTrustMail für Microsoft® Outlook® Version 2.0.1
- Anwenderkomponente SignTrustMail für Lotus Notes® R5 Version 2.0.1
- Signaturanwenderkomponente SecSigner® Version 2.0.0
- Anwenderkomponente eKurier für Microsoft® Outlook® Version 2.0.1
- Anwenderkomponente e-Kurier für Lotus Notes® R5 Version 2.0.1
- Anwenderkomponente SMTP-Proxy für eKURIER Version 2.0.1
- Anwenderkomponente GERVA Version 1.2
- Anwenderkomponente Signatursoftwareprodukt trustview Version 2.1.0
- Signaturanwendungskomponente AVA-Sign Paket
- Anwenderkomponente GERVA Version 1.31 Signaturanwendungskomponente T-TeleSec Signet Version 1.5
- Signaturanwendungskomponente OPENLiMiT SignCubes Version 1.5
- Signaturanwendungskomponente BKK SignCubes Version 1.5
- Signaturanwendungskomponente SignCubes Professional Version 1.5
- Signaturanwendungskomponente e.siqia SignCubes Version 1.5
- Signatursoftwareprodukt Signier- und Verifikations-Anwendung SVA Version 1.3
- Signaturanwendungskomponente S-TRUST Sign-it Basiskomponenten 2.0 Version
- Signaturanwendungskomponente OPENLiMiT SignCubes Basiskomponenten 2.0 Version 2.0.1.1
- Signaturanwendungskomponente OPENLiMiT SignCubes Basiskomponenten 2.0, Version 2.0.1.1 mit OPENLiMiT SignCubes PDF Plugin Version 2.0.1.1 für Adobe
- Signaturanwendungskomponente BKK OPENLiMiT Basiskomponenten 2.0 Version 2.0.2.1
- Signatursoftwareprodukt Signier- und Verifikations-Anwendung SVA Version 1.4
- Signaturanwendungskomponente S-TRUST Sign-it Basiskomponenten 2.0 Version 2.0.3.1

---

[366] cf. Federal Networking Agency, Products for qualified electronic signatures, signature application components, http://www.bundesnetzagentur.de/enid/409c64ff38ce239a1936c1ff8c37a425,0/Produkte/Signaturanwendungskomponenten_vv.html, access on 14.11.2007, 19:19

- Signaturanwendungskomponente multisign Enterprise, Version 3.1.1.3
- Signaturanwendungskomponente DATEV Anwenderkomponente GERVA, Version 1.4
- Signaturanwendungskomponente S-TRUST Sign-it
- Basiskomponenten 2.1 Version 2.1.5.1
- Signaturanwendungskomponente OPENLiMiT SignCubes Basiskomponenten 2.1 Version 2.1.1.1
- Signaturanwendungskomponente Signtrust Signaturserver, Version 3.1.1.3

•Operation Libraries:

- Funktionsbibliothek TCrypt-TCM, Version 1.0
- SafeGuard Sign&Crypt, Version 2.0
- Signtrust Signierkomponente SK-DPAG Version 1.0.
- SafeGuard Sign&Crypt Software Development Kit Vers. 2.0
- Funktionsbibliothek DATEV Signierkomponente DVSigE2, Version 1.0
- Funktionsbibliothek DATEV Signierkomponente DVSigE2, Version 1.1
- Funktionsbibliothek SECUDE, Version 6.0.1
- Funktionsbibliothek TCrypt-SigG, Version 1.3
- Funktionsbibliothek SECUNET Signierkomponente Version 1.0 Funktionsbibliothek TC-SigPK, Version 1.0
- Funktionsbibliothek DATEV Signierkomponente DVSigE2, Version 1.2
- Funktionsbibliothek SECUNET Signierkomponente Version 1.1
- Funktionsbibliothek SECUNET Signierkomponente Version 1.2
- ArtSignComponent Version 1.0
- Funktionsbibliothek DATEV Signierkomponente Trustcenter DVSigKompTC, Version 1.0
- Funktionsbibliothek IAIK-JCE CC Core, Version 3.1
- Signatursoftwareprodukt Signier- und Verifikations-Anwendung SVA Version 1.3
- Funktionsbibliothek Signier- und Prüfkomponente TC-SigPK, Version 1.1Funktionsbibliothek LibSigG, Version 4.7.1.0
- Funktionsbibliothek multisign, Version 4.7.1.0
- Funktionsbibliothek TCrypt-TCM, Version 2.0*
- Funktionsbibliothek secunet Signierkomponente, Version 1.4
-

Application programming interface for online-verification

To check the validity of certificates, OCSP, CRL and LDAP services are offered in Germany.[367]

[367] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile France, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

2.10.4 Summary

Table 36 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 36: Summary and rating, Germany, source: own illustration

categories		rating
legal framework	Germany was one of the first countries to adopt an Electronic Signaure Law in 1997. Further technical specifications are reguleted by the corresponding signatur ordinance.	A
technical standard	eGov, eInvoice eTax eGovernment initiative was one of the most momentous initiatives in Europe all types of electronic signatures, qualified certificates, qualified timestamp, several types of cardreaders, huge range of service providers, most of them accredited CRL, OCSP, LDAP	A
distribution	To sign eInvoices electronically high investments must be mad, thus mass signatures are only rentable for large firms. About 25.000 qualified certificates on secure signature creation devices have been issued.	B

2.11 Greece

Figure 42: Fact-sheet: Greece, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 42 some basic demographic and geographic data of the country is presented.

2.11.1 Institutional frame

Legislation

The EU Directive 1999/93 was implemented in Greek by the Presidential Degree 150/2001[368] (see Appendix - Greece: Presidential Degree 150/2001.[369]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Greece: National Regulations Details.[370]

•recognition of foreign certificates:[371]

In March 1998, the agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:

Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great

[368] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

[369] cf. http://nomothesia.ependyseis.gr/eu-law/getFile/ΠΔ+150+2001.pdf?bodyId=500, access on 26.06.2007, 18:55

[370] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[371] cf. Study of the Donau Universität Krems, Master-Studie, Austria

Britain, Canada and the USA. Currently (status June 2006) 24 States have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of Online Services

•eGovernment

The „Citizen Service Centers“ (KEP) are the administrative service centers where citizen can access information and over 1000 standardized services. This network is also represented online by the platform e-KEP, where the centers are linked electronically and use an uniform platform to manage citizens‘ request, access the eDirectory, use mail etc. The KEP-Platform enables on-line transactions between administration authorities by supporting certified digital signature. The platform design is shown in figure 43.

KEP has more than 9 million visits per month and more than 60 000 citizens access the service centers for transactions with the greek government.

Since March 2007, also Greek enterprises can make transactions with 59 Chambers quickly and easily.

Currently, 1036 „Citizen Service Centers“ are spread around Greece and 1014 administrative procedures can be accessed.[372]

Figure 43: e-KEP, Greece, source: http://www.kep.gov.gr/portal/page/portal/MyNewPortal?lng=us, access on 10.1.2007, 09:24

[372] cf. ePractice.eu, eGovernment Factsheet - Greece - National Infrastructure, 14 December 2007, http://www.epractice.eu/document/3368, access on 10.1.2007, 09:12

Another government portal is under development - Hermes. This project plans to provide citizen and businesses with 300.000 smart cards for effecting transactions with the public sector.[373]

•SYZEFXIS - Public Sector Networks:
Using electronic signature secures data exchange and electronic transaction between public administration authorities. A Public Key Infrastructure will be provided by the Administration Network SYZEFXIS. Since January 2006 a pilot project is tested.
In this connection, about 50.000 smart cards and 10.000 smart card readers are distributed to citizens. These smart cards contain two different digital certificates and should easier the operability between public sector agencies and applications. [374]
In addition to that 2.000 SSL Certificates are issued to certify government services.
Authentication and signature relies on electronic certificates. [375]

A list of operational and planned applications in the eGovernment sector can be found in the Appendix - Greece: Operational and planned applications. [376]

Types of electronic signature
The electronic signatures used in Greece, in accordance with the Presidential Degree, are:

- basic (simple) electronic signature,
- advanced electronic signature or digital signature,
- advanced electronic signature based on a qualified certificate and created by a secure signature creation device. [377]

The SYZEFXIS system relies on qualified signatures based on certificates on smart cards or USB tokens.[378]

2.11.2 Application requirements

Types of certificates
In Greece, there are two types of certificates:

[373] cf. ePractice.eu, eGovernment Factsheet - Greece - National Infrastructure, 14 December 2007, http://www.epractice.eu/document/3368, access on 10.1.2007, 09:12

[374] cf. ePractice.eu, eGovernment Factsheet - Greece - National Infrastructure, 14 December 2007, http://www.epractice.eu/document/3368, access on 10.1.2007, 09:12

[375] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Greece, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[376] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Greece, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[377] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

[378] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Greece, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

- common digital certificates,
- qualified certificates.[379]

Qualified certificates can either be created in a secure signature creation device (hardware) or in the user's browser (software certificate). Common digital certificates are both hardware and software certificates.[380]

The smartcards that are issued in context of SYZEFXIS contains two digital certificates, one for electronic signature creation and one for cryptography procedure. The certificates comply with the X-509 standards. The fields of the certificates are listed up in the Appendix - Greece: Fields of the Certificate.[381]

The types of certificates offered by ADACOM are:

- common certificates (Class 1 VeriSign certificates): individual certificates, subscriber's distinguished name is unique and unambiguous within the CA's Subdomain, certain eMail address is associated with public key, for digital signatures, encryption and access control for non-commmercial or low-value transactions, use of secure signature creation device is not required.
- Qualified certificates: highest level of assurance, issued to individuals, used for digital signatures, encryption, access control, proof of identity in high-value transactions, use of secure signature creation device is required.
- Class 3 organizational certificates (server certificates, SSL): issued to devices to provide authentication, message, software and content integrity, confidentiality encryption.[382]

Up to now, ADACOM S.A. has issued about 2.350 Class 1 Certificates, 300 qualified certificates and 1.900 server certificates. [383]

ADACOM S.A. was approved by the Czech Arbitration Court, in order to provide electronic signatures to European users that seek to resolve disputes regarding .eu domain names. ADACOM S.A was listed as the first and, at present, the only Certification Service Provider in Europe, with products that have been successfully tested for compliance with on-line platform of the Czech Arbitration Court. For more information see http://www.adr.eu/adr/electronic_signatures/index.php.[384]

---

[379] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

[380] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

[381] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Greece, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[382] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece, for more information also see: http://www.adacom.com/index.php?option=com_content&task=category&sectionid=7&id=22&Itemid=40

[383] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece,

[384] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece,

Certification Service Providers

Currently, seven certification service providers are registered within the Hellenic Competent Supervisory Authority, three of them issuing qualified certificates.[385]

➡Short description of Adacom:[386]

ADACOM S.A., founded in 1998, subsidiary of Ideal, is the leader in PKI Services and Information Technology Security. As a VeriSign Certified Affiliate, ADACOM implements Certification Services for the Greek, Cypriot and Balkan markets. ADACOM's philosophy as an end-to-end solution provider is completed through the offer of products and services in the areas of Network security, Content Security and Smart Card Applications in co-operation with leading vendors such as Check Point, G&D, Symantec, and Omnikey. ADACOM complies with Greek, European and international standards and legal requirements and is ISO 9001:2000 certified. Through its authorized network of strategic partners ADACOM has implemented solutions for the largest organizations in Greece and Romania, expanding rapidly to the other Balkan countries and Cyprus.

ADACOM belongs to VeriSign International Affiliate Trust Network. It has satisfied the stringent security conditions and invested the necessary resources to build the first Processing Center in the Balkan area. The height of the investment exceeds 7 Mil. Euro to date. Adacom is registered since 2002 in the Registry of the Hellenic Telecommunications & Post Commission (EETT) as CA Provider for Qualified Certificates.

ADACOM is the exclusive PKI Services Provider for the Greek Public Sector since the completion and delivery of SYZEFXIS Sub-project No.9 on 31/12/2005. ADACOM is currently designing and implementing the E-Citizens project (HERMES), for the Greek Ministry of Interior. In addition, ADACOM has been listed as the first Certification Service Provider in Europe, with products that have been successfully tested for compliance with the on-line platform of the Czech Arbitration Court, for the ADR.eu.

ADACOM offers services for the whole certificate life-cycle. More specifically, ADACOM provides issuing, managing, renewing and revoking certification services.

Additionally, ADACOM offers outsource PKI services (MPKI Services) for private and public organizations. On customer's request, ADACOM provide OCSP services, suspension services and key escrow services, as well.

➡ Short description: Hellenic Public Administration Root Certification Authority

It was established in March 2006 and belongs to the Ministry of Interior. It defines policies and coordinates other public agencies providing certification services.[387]

The other certification service providers are

- EFG Eurobank ERGASIAS BANK S.A.

---

[385] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

[386] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

[387] cf. ePractice.eu, eGovernment Factsheet - Greece - National Infrastructure, 14 December 2007, http://www.epractice.eu/document/3368, access on 10.1.2007, 09:12

- Ahtens Chamber of Commerce and Industry (EVEA)
- EDPS SA
- ATHENS EXCHANGE S.A.
- GENIKI Bank of Greece SA

Table 37 lists up all certification service providers in Greece:

Table 37: Certification Services Providers in Greece, source: own illustration

Certification Service Provider		Issued Certificates
Adacom		Class 1 Certificates Qualified Certificates SSL Server Certificates
Eurobank EFG		no Qualified Certificates
Athens Chamber Commerce and Industry		no Qualified Certificates
EDPS SA		no Qualified Certificates
Athens Exchange S.A.		Qualified Certificates
Hellenic Public Administration Root Certification Authority		Qualified Certificates
Geniki Bank		no Qualified Certificates

A voluntary accreditation scheme has not currently been implemented in Greece. Thus there are not voluntary accredited certification service providers in Greece.[388]

Inspecting authorities

The Hellenic Telecommunications & Post Commission (EET) supervises the certificate service providers and regulates telecommunication and postal services in Greece.

2.11.3 Technical preconditions

Signature software

n.a.

Types of secure signature-creation device

Adacom offer secure signature creation devices that comply with the European and Greek legislation. Specifically, Adacom offers Giesece&Devrient (G&D), Aladdin and Athena USB Tokens and Smart Cards.[389]

[388] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

[389] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

All supported products by Adacom are listed up in table 38:

Table 38: Supported Smart Cards and Tokens by Adacom, source: http://www.adacom.com/index.php?option=com_content&task=category&sectionid=7&id=60&Itemid=78, access on 13.11.2007, 11:02

Type	model	
G&D	SmartC@fe Starkey 400	
	Bio Token	
	SmartC@fe Smart Card	
	Starkey 100	
	STARCOS 3.0	
Athena	ASEKey Crypto USB Token	
	ASECard for Windows	
	ASEKey Crypto J USB	
	ASECard Crypto J	
Aladdin	eToken PRO Smartcard	
	Etoken Pro USB	

Usually, secure signature Creation Devices require a PIN entry in order to get access.[390]

The SYZEFXIS system relies on qualified signatures based on certificates on smart cards or USB tokens.[391]

Card readers

Adacom offers the following smart card readers, that do not require a PIN entry (table 39):

Table 39: Card readers in Greece, recomended by Adacom, source: Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens[392]

type of card readers	mark (models)		connection	supporting operation systems	remark
OmniKey	CardMan 4321 ExpressCard™ 54		ExpressCard 54mm	Windows 98/ME, Windows 2000, Windows XP, Windows 2003 Server, Windows XP64bit (IA64, AMD64, EM64T), Linux	

[390] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

[391] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Greece, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[392] for more information see: http://www.adacom.com/index.php?option=com_content&task=category&sectionid=7&id=29&Itemid=91, access on 09.08.2007, 09:19

type of card readers	mark (models)		connection	supporting operation systems	remark
	CardMan 4040 PCMCIA		PC-Card Type II (PCMCIA)	Windows 98/ME, Windows 2000, Windows XP, Windows Server 2003, Windows XP64bit (AMD64, EM64T), Windows Vista, Windows CE (depending on hardware), Linux, Mac OS X	
	CardMan 3121 USB		USB 2.0 (Universal Serial Bus)	Windows 98/ME, Windows 2000, Windows XP, Windows Server 2003, Windows XP64bit (IA64, AMD64, EM64T), Windows Vista 32bit, Windows Vista 64bit, Windows CE (depending on hardware), Linux, Mac OS X	
	CardMan 3021 USB		USB 2.0 (Universal Serial Bus)	Windows 98/ME, Windows 2000, Windows XP, Windows Server 2003, Windows XP64bit (IA64, AMD64, EM64T), Windows Vista 32bit, Windows Vista 64bit, Windows CE (depending on hardware), Linux, Mac OS X	
Keyboards (Cherry)	G83-6644		USB 2.0		
	G83-6744 Smart Card Keyboard				Secure PIN entry (class 2 reader)
	G83-14201 Biometric Keyboard with Smart Card Reader		USB		USB keyboard with fingerprint sensor and PC/SC smart card reader AuthenTec AES CMOS Fingerprint Sensor with TruePrint® Technology CardMan 3121-compatible Smart card reader
	G83-14401 Biometric Keyboard with Smart Card Reader		USB		USB keyboard with fingerprint sensor and PC/SC smart card reader Capacitive fingerprint sensor TCS1CD from UPEK (ST-Micro) with TouchChip® technology 256x360 pixel CardMan 3121-compatible Smart card reader
	AP POS G81-8040 Keyboards			Windows, Linux, Macintosh	Multifunctional USB Keyboard with integrated Magnetic Card Reader and PCSC & EMV Compatible Smart Card Reader
	AP POS G81-7040 Keyboards			Windows. Linux, Macintosh	Multifunctional USB Keyboard with integrated Magnetic Card Reader and PCSC & EMV Compatible Smart Card Reader

Certificate requirements

Adacom signatures are compatible with the X-509 standard according to RFC 3280. Physical person's certificates are compatible with any e-mail applications and systems that support S-MIME protocols.[393]

Application programming interface for online-verification

ADACOM provide Certificate Revocation List and directory services. On customer's request, they also provide Premium CRL services and Online Certificate Status Protocol services.[394]

2.11.4 Summary

Table 40 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 40: Summary and rating, Greece, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2001.	A
technical standard	eGov, all types of electronic signature common certificates, qualified certificates (hard- and software smartcards or USB token, ID cards under construction, several types of cardreaders recommended, no accredited CSP, 7CSP (3 issue qualified certificates CRL, OCSP	B
distribution	The online platform of the Citizen Service Centers supports certified digital signature and is accessed by more than 60.000 ciitzitens per month for transactions with the Greek government. pilot project for electronic transactions between public administration authorities: distribution of 50.000 smartcards and 10.000 readers by SYZEFXIS for Public Key Infrastructure issuance of 2.000 SSL Certificates for government services ADACOM issued 2.350 basic, 300 qualified and 1.900 SSL certificates	A

[393] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

[394] cf. Correspondence with Despina Dimitra, Certificate Policy Manager, Adacom S.A., Athens, Greece

2.12 Hungary

Figure 44: Fact-sheet: Hungary, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:50

In figure 44 some basic demographic and geographic data of the country is presented.

2.12.1 Institutional frame

Legislation

A Law on electronic signatures exists since the late ´90s.

The directive was implemented into law on the 12th June 2001 (Act No 35 of 2001 on electronic signatures), and entered into force on 1st September 2001. It was significantly amended in 2004.[395]
The Law can be found in Appendix - Hungary: Act on electronic signatures.[396]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Hungary: National Regulations Details.[397]

•recognition of foreign certificates:[398]
In October 1998, the agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 States have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,

[395] cf. Correspondence with Dr. Szilveszter Adam, National Communication Authority, Hungary

[396] cf. http://www.nhh.hu/dokumentum.php?cid=10623, access on 28.11.2007, 12:38

[397] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[398] cf. Study of the Donau Universität Krems, Master-Studie, Austria

- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of online services

•Internet access:[399]

In Hungary, the popularity of Internet use is limited. In 2002, 85% of the population rejected the Internet, in 2005, 60% of all households were not using it. In December 2005, a report was published by the Austrian Fessel-GFK[400]: hence, Hungary was 29th of 37 surveyed European countries with only 33.2 % of the population alder than 15 years had access to the Internet, which means 8.5 million people.

But the figures are rising. Between 2000 and 2006, the Internet users increased for 3.3 and by June 2006, about 1 million people had Internet access.

•eGovernment:[401]

eGovernment had to face a lot of obstacles, like digital differences in the country and the limited use and access of Internet.

Since the early 90ies, the organizational unit eGovernment Center (since 2003) of Prime Minister's Office is responsible for the coordination and development of eGovernment in Hungary. In 2003, an eGovernment Strategy „eGovernment 2005" was launched. 27 services of 17 institutions can be accessed through the government portal and the Client Gate (http://www.magyarorszag.hu, figure 45). Until November 2006, over 380.000 people haver registered. Users can log in with user name and Pin code, but also may us a qualified certificate for their registration.

Figure 45: eGovernment Portal Hungary, source: http://www.magyarorszag.hu, access on 28.11.2007, 12:38

[399] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[400] see http://www.gfk.at

[401] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

The Interdepartmental Committee for IT of the Prime Minister‘s Office was the first to take initiative for using electronic signatures in 1994 and promoted smart cards. Therefore a Smart Card Forum was established 3 years later. But there are only A2A and B2B applications that use electronic signature and they do not require qualified certificates. For the Client Gate, PIN code authentication was used and the tax declaration systems use PKI based time stamping services.[402]

•eBev - electronic tax declaration system:[403]
In 2000, the first electronic tax declaration system was developed, using hand written signature, installed for 500 large Hungarian companies.
In 2004, a new system started for 3.000 enterprises, including downloadable forms, special software tools, using electronic signatures. During the oncoming year, thy system was enlarged to 10.000 taxpayers. All in all, about 23.000 certificates were issued. Since 2006, the etax system is accessible trough the eGovernment portal‘s Client gate. Since January 2007, the system can be used by all tax payer using all kinds of advanced electronic signature based on certificates of any commercial CSP that is certified by the Public Administration rootCA.
The forms for the tax declaration system along with the needed software can be downloaded at http://www.apeh.hu/bevallasok/nyomtatvany/bevallasok.The software enables to fill out the forms and submit them to the Tax and Financial Control Administration via the Client Gate of the eGovernment Portal.

•eHealth[404]

- Janlent:
  Employers must declare the employees data to the National Health Insurance Found OEP405. Therefore, a system for the declarations of persons entitled for health insurance was developed that enables an electronic submission of data. The Files are generated y the client program Jalent. Electronic signatures ensure integrity, authenticity and security of the data transmitted by te user. The files are encrypted and sent as e-mail attachment, signed with an advanced electronic signature. Each month, about 1.500 declarations were sent by about 3.000 firms.
  The monthly number of reports that are received since January 2006 is shown in table 41.

Table 41: monthly distribution of the reports, received, source: European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, source: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Month	Reports (number)
1	4
2	47

[402] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[403] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[404] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[405] see http://www.oep.hu

Month	Reports (number)
3	193
4	379
5	602
6	919
7	943
8	1164
9	1397
10	1505

- The required certificate for advanced or qualified signature can be issued by any Certification Service Provider that is registered at the National Communication Authority. The Client program Jelent can be downloaded from http://www.oep.hu/portal/page?_pageid =35,283051&_dad=portal&_schema=PORTAL#jelentprogram .
  The system is operating since January 2006 and the number of declarations sent electronically rises month by month.
- DSend:
  One of the first and largest application nation wide in Hungary was the electronic data reporting of patients and their medical attendance. Hospitals, health institutions, doctors and health service providers can report data of medical attendance with help of the application DSend. By using electronic signature integrity authenticity and security of data is assured. DSend uses advanced certificates of an authorized certification service provider. The partners are connected via a closed messaging system and use advanced electronic signature for a non-repudiation, integirty rights management. Furthermore, time stamps are used.
  Currently 65 clients use the system.

•Electronic Declaration System for Private Pension Found:[406]

Employers must submit their pension fund declarations regularly o the Administration of National Pension Insurance[407] and to private pension funds if they are members of one. Those private funds submit all data to the Central Register of Pension Funds that is managed by the Hungarian Financial Supervisory Authority.[408] The employers complete the declarations, signed with qualified electronic signature and provided with a time stamp. The software and encryption keys can be downloaded at http://www.pszaf.hu/engine.aspx?page=pszafhu_letoltesek_infok. Digital certificates and time stamps can be obtained from any certification service provider.

The pension funds receives about 400-700 electronic declarations each month. But there are also problems due to different certification renewals and a lack of common certificate profiles.

The declaration system is the fits application that uses the services of the certification service providers in large scale.

[406] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[407] see http://www.onyf.gov.hu

[408] see http://www.pszaf.hu/

•other eServices:
Hungary plans further applications for eGovernment services that are listed up in detail in the Appendix - Hungary: Operational and planned applications for eGovernment services, including Online services of the Citizens' Gate for enterprises and citizens or applications at local level.

Types of electronic signature

The function of electronic signatures has not been widely used.
Even Government tries to get around using them and has developed other solutions for authentication and identification.
The reason why they are not being used is that for many forms, a countersignature of a lawyer or a notary is necessary, so the use of electronic signature is surplus.[409]

The law is discerning three main areas:Basic, advanced and qualified. Basic digital signature isn't prove anything, it's like inserting my name to the end of this e-mail. [410]

If a certificate issued for someone for an advanced digital signature purposes, then it can prove his/her identity. It's equal with the traditional handwritten signatures, so the receiver has to accepted it and can not ignore it just because it's a digital one. If there is any debate with the advanced digital signature - just like in the past - the court has to resolve the problem. However, the signer has to prove he/she made the digital signature.

Qualified digital signature is the strongest electronic signature in Hungary. It's like the same if someone creates a signature in front of two whiteness. So after this qualified digital signature created on the document, it'll became a private document representing conclusive evidence. If there is any debate with the qualified digital signature, the person who has any doubt with it has to prove its invalidity at the court.[411]

Of the three classes, probably the basic electronic signature is used the most because it has no specific requirements. However, signers are often not aware when they are using it (e.g., just by writing their name under an email) The use of advanced and qualified signatures is much more restricted. Of the two, advanced signatures are the ones that are used more, qualified signatures are mostly only used where it is mandatory to do so.[412]

A register of all eSignatures can be found on the site http://webold.nhh.hu/esign/kozig/init.do.[413]

Examples for the adoption of electronic signatures are the eGovernment Client Gate using qualified signature, the electronic tax declaration system eBev using at least advanced electronic signature, or the

[409] cf. Business Hungary (2007)

[410] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

[411] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

[412] cf. Correspondence with Dr. Szilveszter Adam, National Communication Authority, Hungary

[413] cf. Correspondence with Zoltan Vegh, IT Manager, MAV Informatika Plc., Hungary

electronic social security applications: The system Jelent uses advanced or qualified electronic signature, DSend requires advanced electronic signature.[414]

But electronic signatures are not widely used in Hungary. Of the 390.000 users that are registered for the eGovernment Client gate only 63 use electronic signature for authentication and log in.
The qualified electronic signature is expensive and not user friendly. Instead of PKI technologies other solutions would be preferred when using a cost benefit analysis. In addition, the level of Internet penetration does not deliver a basis for a roll-out and offer of common applications of electronic signatures.[415]

2.12.2 Application requirements

Types of certificates

The Act on electronic signatures regulates two kind of certificates that are issued to the public with the aim of the verification of electronic signatures.

- One is the qualified certificate. This kind of certificate must be issued by a certification service provider that has either been registered in Hungary as a qualified service provider or is accepted as equivalent by the Act. (The recognition of qualified certificates from other countries follows the rules set out by the electronic signatures directive) These certificates follow the requirements laid down in the relevant internationally accepted standards documents by ETSI and other bodies (e.g., by specifying a qualified certificate statement) for their structure and content.
- The other is the non-qualified certificate. This can be issued by any certification service provider that is registered in Hungary or any other provider from a different country that has been recognized as equivalent by the Act. These certificates can be distinguished e.g., by looking up the Certification Policy that is indicated in the certificate. These certificates also follow internationally accepted standards documents for structure and content.[416]

Both qualified and non-qualified certificates can be issued either for hardware-based or for software-based key tokens. However, qualified signatures can only be prepared using a secure signature-creation device and must be based on a qualified certificate. If a qualified certificate is used without a secure signature-creation device, then only advanced electronic signatures can be created. The Certification Policy indicated in the certificates specifies whether the keys must be used in a secure signature-creation device.[417]

---

[414] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[415] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[416] cf. Correspondence with Dr. Szilveszter Adam, National Communication Authority, Hungary

[417] cf. Correspondence with Dr. Szilveszter Adam, National Communication Authority, Hungary

The eGovernment Portal can either be accessed by using user name and Pin code or by using a qualified certificate. But qualified certificates are expensive and not required for most of the eGovernment services. Therefore the Client Gate uses Pin code authentication. The electronic Tax declaration uses PKI based time stamping services.
Currently only 0,017 % of the registered users own qualified electronic certificates.
As the Act on Electronic Signature was enacted, attempts were made to use qualified electronic signatures for eGovernment applications, like for an eTaxing system. But because of inadequate definitions of non-qualified, simple, advanced etc signatures, the legal effect of using electronic signatures remained uncertain. Therefore, the use of electronic signature did not became widespread in public administration. According to the decree 194 of 22 september 2005 on electronic signature use in public administration procedures, the use of certificates in public administration requires a personal, face-to-face registration.[418]

In November 2005, the Hungarian government accepted a law that had been reconsidered in 2004. The law (KET – Administration Treatment Act CXL.) have references to the Administrative area. So, after this when the act has been modified there are two main areas for the certificates usage:[419]

- If someone wants to communicate with the Government he/she has to enroll a certificate from a CA that is KET compatible. It doesn't matter if it's a private, administrative or business person. Only these kind of certificates are accepted in this area. So every Autonomy, Office, etc have to apply for this kind certificate until 2009. (It's called some e-government program).
- The other area is – let it called Business Area – the traditional B2B, B2C. Let say, if a private person wants to communicate genuinely with an other private person or with a company (order a service, etc.). Or someone at a company – like ours – wants to digitally sign an order or contract, then this kind of certificate is perfect.

Because of these differences we have to have both services that means the following: Hungary provides Advanced and Qualified CA for normal usages and Advanced and Qualified CA for Administrative purposes(some part are under construction). It means we need at least four CA just for the digital signatures.[420]

The Certificate profile of a qualified electronic signature certificate for clients of the PKI of the public administration can be seen in detail in the Appendix - Hungary: Certificate profile of qualified electronic signature certificates for clients in the Public Key Infrastructure of the Hungarian Public Administration.[421]

---

[418] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[419] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

[420] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

[421] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

MAV Informatika issues advanced and qualified certificates for electronic signatures and supplies qualified timestamp services as well. Up to now, MAV Informatika has issued 920 advanced certificates, 2500 qualified certificates, 520 certificates for security services and around 1.750.000 qualified timestamps.[422]

Tables 42 and 43 show the number of valid advanced and qualified certificates of MAV Informatika Plc. on 1.1.2008, by types and customer groups:[423]

Table 42: Number of valid non-qualified (advanced) certificates for electronic signature on 01.01.2008 by types and customer groups, source: Correspondence with Zoltan Vegh, IT Manager, MAV Informatika Plc., Hungary

Issued for	Private (personal)	Corporate associate	Corporate organizational
Private Individual	12	-	-
Corporate	-	400	5
Government	-	233	-
other	-	137	-
Sum Total	12	770	5

Table 43: Number of valid qualified certificates for electronic signature on 01.01.2008 by types and customer groups, source: Correspondence with Zoltan Vegh, IT Manager, MAV Informatika Plc., Hungary

Issued for	Private (personal)	Corporate associate
Private Individual	7	-
Corporate	-	242
Government	-	1
other	-	21
Sum Total	7	264

The number of customers, using electronic signature services (01.01.2008) is shown in table 44.

Table 44: Number of customers for Electronic signauture services on 01.01.2008, source: Correspondence with Zoltan Vegh, IT Manager, MAV Informatika Plc., Hungary

Issued for	Non-qualified (advanced)	Qualified
Private Individual	12	7
Corporate	198	28
Government	120	1
other	96	5
Sum Total	433	41

Tables 45 and 46 show the Certificate Profile of MAV INFORMATICA.

[422] cf. Correspondence with Zoltan Vegh, IT Manager, MAV Informatika Plc., Hungary

[423] cf. Correspondence with Zoltan Vegh, IT Manager, MAV Informatika Plc., Hungary

Table 45: certificate profiles of MÁV INFORMATIKA Ltd., not for public administration, source: Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

General usage (not for public administration	Qualified Digital Signature	Advanced Digital Signature	Encryption	User Authentication
Private persons	yes	yes	yes	yes
person representing an organism (organizational person)	yes	yes	yes	yes
organization	no	yes	yes	yes
automatism representing an organism (hardware, like: routers, web servers, etc.)	no	yes	yes	yes

Table 46: certificate profiles of MÁV INFORMATIKA Ltd. for public administration, source: Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

KET (Public Administration)	Non-repudiation (only signature), Qualified	Non-repudiation (only signature), Advanced	Encryption	User Authentication
Administrators of a Public Administration - Public Sector Administrator	yes	yes	yes	yes
An automatism which represents a Public Administration - server	no	yes	yes	yes
Customers of Public Administration – Private Person or Public Sector Administrator	yes	yes	yes	yes
mechanisms run by clients getting into contact with Public Administration - server	no	yes	yes	yes

According to the latest statistics on 1st January 2008, 8.193 valid certificates have been issued to the public. Of these 8.193 certificates, 3.441 were non-qualified and 4.752 qualified certificates.
In 2007, 1.373 certificates have been issued on secure signature-creation devices.
Between 2005 and 2007, 3.294 certificates have been issued on secure signature-creation devices in total.[424]

Certification Service Providers

There are currently some certification service providers registered in Hungary, issuing certificates to the public. There is no voluntary accreditation scheme in Hungary. All of them are accredited an audited by NHH (National Communication Authority) which represents the Government and audited by an independent person.[425]

Currently, there are 6 Certification Service Provider in operation, 4 of them issue qualified and non-qualified certificates, 2 issue only non-qualified certificates.[426]

[424] cf. Correspondence with the National Communications Authority, Directorate of General Inspection, Department for Customer Relations and Information, Hungary

[425] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

[426] cf. Correspondence with National Communications Authority, Directorate of General Inspection, Department for Customer Relations and Information, Hungary

➡Short description: e-Szigno Certificate Authority
e-Szigno operates as a Certification Authority and issues digital certificates. They offer different certificates, qualified certificates for digital signature, non-qualified certificates for digital signature, Encryption and user identification.[427]

➡Short description: MÁV INFORMATIKA Ltd.
MÁV INFORMATIKA Ltd. is owned by the Hungarian Railway Company (which is owned by the government). Around 500 employees work for the company and we have national presence (6 county branch office, plus the headquarter in Budapest).

After the Government has implemented et EU directive in the Hungarian legislation, the company decided to be involved in this area, started PKI services in 2001 and became an Advanced CA in November 2002. in parallel with that they started a TimeStamp service. In the next year MÁV INFORMATIKA Ltd. becomes an Qualified CA as well.[428]

➡short description: Netlock
Also Netlock offers qualified certificates to the public.

➡short description: Magyar Telekom Nyrt
Also Magyar Telekom Nyrt offers qualified certificates to the public.

➡short description: Ministry of Informatics and Communications, Security Certification Authority
Also the Ministry of Informatics and Communications, Security Certification Authority offers qualified certificates to the public.

Table 47 lists up all certification service providers in Hungary.

Table 47: Certification Service Provider in Hungary, source: own illustration

Certification Service Provider		Issued Certificates
Ministry of Informatics and Communication www.bhsz-m.gov.hu		qualified certificates
Magyar Telekom Communication AG. www.magyartelekom.hu	Magyar Telekom	n.a.
Microsec Computing Development Ltd www.e-szigno.hu	microsec e-szigno	qualified certificates non-qualified certificates

[427] cf. http://www.e-szigno.hu/index_de.html, access on 25.07.2007, 19:13

[428] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

Certification Service Provider		Issued Certificates
MÁV INFORMATIKA Ltd www.mavinformatika.hu	MÁV INFORMATIKA Kft.	qualified digital signature advanced digital signature
Netlock Ltd. www.netlock.hu	NETLOCK	Personal Certificates Qualified certificates Server Certificates

Inspecting authorities

The five national trust service providers are supervised by the National Communication Authority[429] that controls the fulfillment of the requirements of the Act on electronic signatures and of the implementing regulations.

The bodies, responsible for the determination of conformity of the secure signature creation devices according to Art. 3.4 of Directive 1999/93/EC are:

- Hunguard Kft. and
- Matrix Vizsgáló, Ellenõrzõ és Tanúsító Kft.

2.12.3 Technical preconditions

Signature software

To create qualified digital signature you have to have a Qualified Application for signing documents. (There is a list of the approved application on the National Communication Authority's – NHH's site). Anyone can develop this kind of software, it just has to be tested, audited and approved by NHH. There is no rule for operating system.[430]

Types of secure signature-creation device

Secure signature-creation devices are the Hungarian eID card, HUNEID.

The eGovernment Client Gate relies on qualified signatures for registration to use different electronic services. Different kind of signature-creation devices can be used, like smart cards or USB Token, delivered by the certification service providers.
The electronic Social Security Application Jelent requires advanced electronic signatures on smart cards or software certificates, DSend requires advanced electronic signature on smart cards.
The Electronically authenticated private pension fund declaration system requires qualified signature certificates on Smartcards.[431]

---

[429] cf. http://www.nhh.hu/index.php, access on 08.08.07, 11:41

[430] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

[431] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

MÁV INFORMATIKA Ltd. is issuing advanced certificates on soft-keys, usually on floppy, CD-ROM or other devices. MÁV INFORMATIKA Ltd. is using only Giesecke&Devrient StarCOS smartcards for qualified and Oberthur CosmopolIC, Aladdin eToken, Giesecke&Devrient SafeSign, G&D StarKey 100 token for advanced signatures. But, they support other smart cards as well, (which have a proper pkcs11 library).[432]

Card readers

The usage of Class-2 or 3 card readers is not expected, however if the user wants to have a higher security level can use it. If the eGovernment project will run up, the usage of these kind of smart-card readers will be spread out.[433]

Certificate Requirements

The electronic tax declaration system eBev that enables taxpayers to submit their tax declarations electronically to the Tax and Financial Control Administration, requires a special software tool. This software can be downloaded from http://www.apeh.hu/bevallasok/nyomtatvany/bevallasok. After installation the forms can be filled out and submitted to the Tax and Financial Control Administration.[434]

For electronic submission of declarations for the National Health Insurance Found the system Jelent was developed. The system requires a client program that encrypts and sends data as e-mail attechment signed with advanced qualified electronic signature. This Client can be downloaded at http://www.oep.hu/portal/page?_pageid=35,283051&_dad=portal&_schema=PORTAL#jelentprogram and must be installed on the PC of the user. Requirements are the operation system MS Windows 2002 or higher, an E-mail software, a smart card to create the signature, the card reader or instead of those a software certificate.[435]

Another social security application is DSend, a system to report medical attendance of patients. Different health institutions are connected via a management system and assure a secure data exchange by using advanced electronic signature certificates. The basic requirements for implementing and operating DSend are:

- Windows 2000, Windows XP, Windows 2003
- smart card
- certificate management program

[432] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

[433] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

[434] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[435] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

- DSend Client Program.[436]

The electronic pension fund declaration system enables to submit declarations electronically, signed with a qualified signature and provided with a time stamp. The software modules of the program that enables data submission along with encryption keys can be downloaded at http://www.pszaf.hu/engine.aspx?page=pszafhu_letoltesek_infok.[437]

Application programming interface for online-verification

MÁV INFORMATIKA Ltd. has CRL and OCSP services as well. The CA must issue CRL in every 24 hours at least one time, and there are couple of fields when the customer requires that service. The customer has to pay for this service.[438]

MÁV INFORMATIKA Ltd. has to issue CRL daily (so in every 24 hours), however has OCSP service for the Qualified certificates and for the Advanced it is under construction.

2.12.4 Summary

Table 48 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 48: Summary and rating, Hungary, source: own illustration

categories		rating
legal framework	A Law on electronic signatures exists since the latest '90s. The EU directive has been implemented in 2001, and was significantly amended in 2004. Electronic signature is not widely used as for many forms, a lawyer or notary is necessary.	B
technical standard	eGov, eTax, eHealth eGovernment strategy, Smart Card Forum all types of electronic signature qualified and non-qualified certificates (hardware and software based) 6 CSP (4 issuing qualified certificates) eID, Smartcard, Token, CRL, OCSP	A

[436] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[437] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Hungary, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[438] cf. Correspondence with Akos Mazan, PKI consultant, Mav Informatika Ltd., Hungary

categories		rating
distribution	The use of Internet is limited in Hungary. Electronic signature is not widely used as for many forms, a lawyer or notary is necessary. Basic electronic signature is used the most as no specific requirement is needed. the use of advanced and qualified signatures is more restricted. of the two, advanced signatures are used more often, qualified signatures are only used where it is mandatory to do so. only A2A and B2B applications use eS and do not require qualified ceritficates for eTax system, about 23.000 certificates have been issued, but only 0,017% use them of the 390.000 useres that are registerded for the eGovernment Portal only 63 use electronic signature for authentication and log-in. Qualified signature is expensive and not user friendly According to the latest statistics on 1st January 2008, 8.193 valid certificates have been issued to the public. Of these 8.193 certificates, 3.441 were non-qualified and 4.752 qualified certificates. In 2007, 1.373 certificates have been issued on secure signature-creation devices. Between 2005 and 2007, 3.294 certificates have been issued on secure signature-creation devices in total.	C

2.13 Ireland

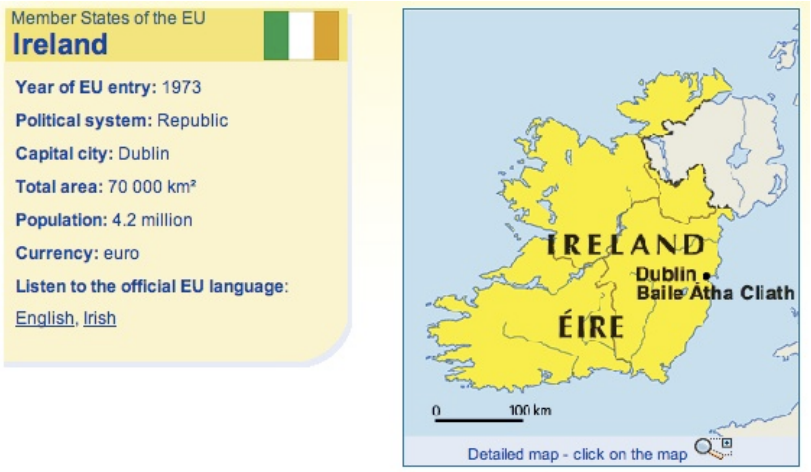


Figure 46: Fact-sheet: Ireland, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:50

In figure 46 some basic demographic and geographic data of the country is presented.

2.13.1 Institutional frame

Legislation

The EU electronic signature Directive 1999/93/EU was implemented into Irish law in 2000 by the Irish E-Commerce Act 2000 (see Appendix –Ireland: eCommerce Act).

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Ireland: National Regulations Details.[439]

Availability of online services

•eGovernment:[440]

The first Action Plan for building an information society in Ireland was published in 1999, covering 3 main areas of public services: information services, interactive online services (like transactions) and integrated services (availability of online services via a single access point of government).

In May 2000, this single point of contact for public services was developed, implemented by Reach agency. In 2001, two portals were implemented to make information available:

[439] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[440] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

- the OASIS website - www.oasis.gov.ie:provides public services information around citizen-centred life events, moved to http://www.citizensinformation.ie/categories. The platform design is shown in figure 47:

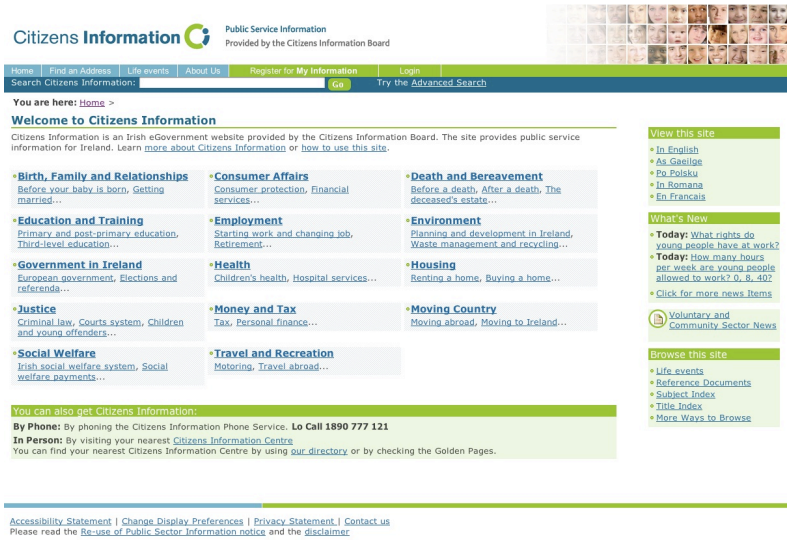


Figure 47: Citizens Information Ireland, source: http://www.citizensinformation.ie/categories, access on 28.11.07, 15:14

- the BASIS website - www.basis.ie: provides public service information around business centered needs (design shown in figure 48):

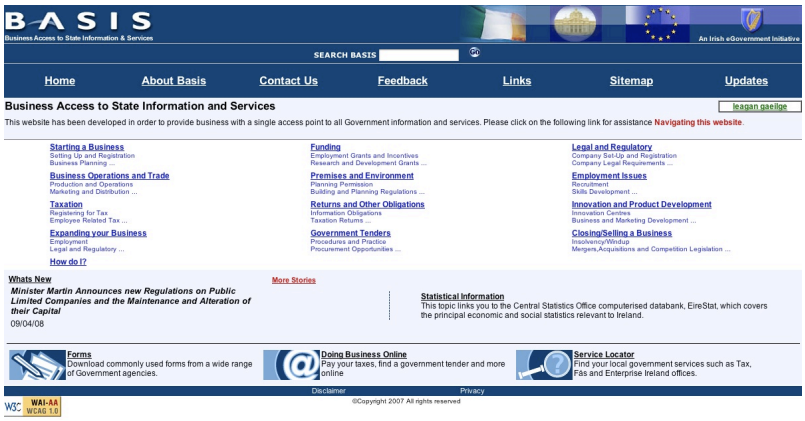


Figure 48: Business Access to State Information and Services, source: http://www.basis.ie, access on 28.11.2007, 15:16

•Reachservices

One example of a key eGovernment site that is currently in place is Reachservices. Launched in 2005, Reachservices is a new portal for public services and the first phase of a broker system. The main page of reachservices is shown in figure 49:

Figure 49: Reachservices Ireland, source: https://www.reachservices.ie/, access on 28.11.2007, 15:21

Reachservices is an public service Broker, providing authentication services as well as a common access point for all eGovernment services for citizens. Furthermore, the site provides a standardized XML based electronic communication for the agency intern. The system was developed in 2002 and provides its interactive services since 2006. It is run by Reach Agency www.reach.ie. Reach Agency was established in 1999 to develop and further public services and eGovernment.
Over summer 2006, a lot of users registered because of the launch of the new services like ROS. Currently about 100.000 users are registered. [441]

•Revenue Online Service ROS:[442]
To enable a secure and electronic billing and paying of taxes, the Revenue Online Service ROS was established in 2002.[443]
ROS relies on qualified signatures based on certificates that are explicitly issued by the Revenue Commissioners for communication with the authority.
In 2005, 290.842 income tax payment transactions have been effected via ROS, about 248.967 income tax self-assessment returns. About 93% of customs declarations have been submitted to the New

[441] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[442] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[443] for more information see http://www.ros.ie/

Computerized Transit System via ROS in 2005. The Transit System automatically validates the declaration for completion of data and codes.

•Companies Registration Office E-Filling system:[444]
The System was established in 2002 for all limited liability companies to enable to fill out, sign and submit their annual returns electronically. For that purpose, ROS acts as its own certification authority, issuing special certificates for the communication between the companies and the authority.
In 2005, 5.4% of the annual returns were submitted electronically. The figures increased from 1.14% in 2003 and from 4.19% in 2004.

•Motor Tax Online:[445]
Since 2003, natural and legal persons can pay their annual motor tax electronically by using their debit or credit cards through a secure server. The responsible organization is the Department of Environment, Heritage and Local Government. This system is widely used and very successful: In 2005, 812.634 transactions have been recorded, in 2006 already 975.000 transactions were effected.

•Other eServices:
Other Important applications of eGovernment are f the Property Registration Authority‘s Land Direct system, the online applications of the Land Registry[446], the Online Redundancy Claim and the Civil Registration Modernization Programme.[447]

Types of electronic signature

Post.Trust has developed a Public Key Infrastructure to enable a private, secure and protected communication for businesses. It is to solve issues concerning securing electronic communication and providing the link to a digital signature. This signature guaranties the integrity of data and documents and validates the identity of the sender.[448]

Certification Europe and the National Accreditation Board of Ireland developed a public accreditation and certification scheme for organizations. This scheme uses PKI systems and assesses the validity of advanced electronic signatures.[449]

---

[444] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[445] cf. ROS acts as its own cercitication authoriy, issuing

[446] for more information see http://www.landdirect.ie

[447] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[448] cf. http://www.post.trust.ie/pki/pki.html, access on 28.07.07, 15:23

[449] cf. Certification Europe Ltd., Qualified Electronic Signatures and Certification, Support of Certification Europe’s Certification Scheme, Fact Sheet June 2003

The eTax system ROS requires a qualified signature based on a certificate that is issued by the Revenue Commissioners explicitly for the communication between the tax payer and the agency. This signature enables to fill out tax returns and pay taxes electronically.[450]

The CRO E-Filling system requires advanced signatures based on qualified certificates that are issued by the Companies Registration office explicitly for the communication between companies and the agency.[451]

The Motor Tax Online System is based on a secure server communication using simple eSignature.[452]

2.13.2 Application requirements

Types of certificates

Post.Trust offers 4 types of certificates:

- qualified digital certificate
- standard digital certificate
- SSL Certs
- CertifID for Adobe Acrobat.[453]

For more technical detail see Appendix - Ireland: digital certificate profile details.

•The Certification Europe Certification Scheme:[454]
Certification Europe and the National Accreditation Board of Ireland developed a public accreditation and certification scheme for organizations. This scheme uses PKI systems and assesses the validity of advanced electronic signatures.

To be certified under that scheme, Certification Service Providers must fulfill four requirements:
1. issuing qualified certificates, supporting advanced electronic signature
2. demonstration compliance with the EU-Directive for electronic signature, Annex I
3. operation an information security management system with recognized standards and
4. demonstrating compliance with the Data Protection Directive 95/46/EC.

•For the eTax system ROS, special certificates are used, that are issued by the Revenue Commissioners explicitly for the communication between the tax payer and the agency.

---

[450] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[451] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[452] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[453] cf. http://www.post.trust.ie/certifid/certifid.html, access on 28.07.2007,15:

[454] cf. Certification Europe Ltd., Qualified Electronic Signatures and Certification, Support of Certification Europe's Certification Scheme, Fact Sheet June 2003 (2003)

To authenticate the user, software certificates or a personal access number are used. The certificate is conform with X.509v3 based certificate standards. To read more about the Certificate, the Certificate Policy Statement of ROS can be found at www.revenue.ie/pdf/pd0039.pdf.[455]

•For the Companies Registration Office CRO E-Filling system, special certificates are issued by the Companies Registration Office explicitly for the communication between the company and the agency. These digital clients certificates are software certificates and an approved secretarial software is required to use the eSignature.[456]

Certification Service Providers

In Ireland, there are currently two certification service providers, namely Post.Trust and Certification Europe.

➡Short description: Certification Europe:[457]
Certification Europe was established in 1999 provides Irish and International markets with independent and confidential certification services.
It was the first Certification Authority in Ireland that offered a service complying with the Information Security Standards BS 7799 / IS 17799 / ISO 17799 and is the only body accredited by the Irish National Accreditation Board (environment standard ISO 14001).

➡Short description: Post.Trust:[458]
Post.Trust, owned by the Irish Postal Authority, is a national level Certificate Authority, responsible for issuing, renewing and managing digital certificates.[459] Post.Trust was founded in 2000 and is an e-business security solution, provided by the Irish Postal Authority, to enable eBusiness in a secure and private environment. It is a national-level Certification Authority issues and manages digital certificates, implemented a PKI solution and developed secure electronic payment solutions.
As Post.Trust is the only digital certificate provider, it has to fully certify all digital certificate holders.

➡short description: Revenue Commissioners:
The Revenue Online Service ROS has its own certification authority. The Revenue Commissioners issues certificates explicitly for the purpose of communication with the agency for ROS.[460]

---

[455] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[456] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[457] cf. http://www.certificationeurope.com/company/default.asp, access on 28.07.07, 19:54

[458] cf. http://www.post.trust.ie/pki/pki.html, access on 28.07.2007, 15:23

[459] cf. http://www.post.trust.ie, access on 28.07.07, 15:22

[460] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

➡short description: Companies Registration:
Same does the Companies Registration Office that acts as its own certification authority and issues certificates for qualified signatures explicitly for the communication with the agency. for the Companies Registration Office E-Filling system.[461]

Table 49 lists up all certification service providers in Ireland:

Table 49: Certification Service Provider in Ireland, source: own illustration

Certification Service Provider		Issued Certificates
Certification Europe http://www.certificationeurope.com/	Certification Europe Ltd	Qualified certificates
Post.Trust http://www.post.trust.ie	POST TRUST Secure e-Commerce Solutions	qualified certificates standard certificates SSL Certificates CertifID for AdobeAcrobat
Revenue Commissioners http://www.revenue.ie/	Revenue	certificates for ROS
Companies Registraion OFfice CRO	cro	certificates for CRO E-Filling

Inspecting authorities

The supervisory authority in Ireland is the Department of Communications, Marine and NAtural Ressources.

2.13.3 Technical preconditions

Signature software

•CertifID for Adobe Acrobat:[462]

CertifID for Adobe Acrobat reader (figure 50) is available at Post.Trust.

Figure 50: CertifID, source: http://www.post.trust.ie, access on 28.07.07, 15:34

[461] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[462] cf. http://www.post.trust.ie/certifid/certifid.html, access on 28.07.07,15:25

With this software you can sign PDFs digitally in Adobe Acrobat reader.

CertifID is a PDF document singing solution that enables to provide a PDF document with a digital signature. So the receiver of a PDF can verify the identity of the sender and trust the origin of the message. To obtain a CertifID certificate from Post.Trust, four steps have to be passed through:

- have identity verified by Post.Trust
- install private signing key
- configure Adobe PDF creator
- sign PDF digitally.

The recipient clicks on a signature icon and retrieves the certification status information (figure 51).

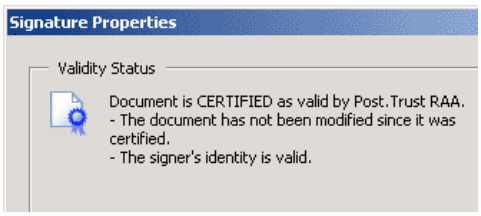


Figure 51: Validity status information, source: http://www.post.trust.ie/certifid/certifid.html, access on 28.07.07,15:25

Types of secure signature-creation device

n.a.

Card readers

n.a.

Certificate requirements

To obtain a CertifID certificate from Post.Trust, four steps have to be passed through:

- have identity verified by Post.Trust
- install private signing key
- configure Adobe PDF creator
- sign PDF digitally. [463]

The software certificates issued by the Companies Registration Office for the E-Filling system requires an approved secretarial software.[464]

[463] cf. http://www.post.trust.ie/certifid/certifid.html, access on 28.07.07,15:25

[464] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Ireland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Application programming interface for online-verification

Post.Trust publishes a Certificate Revocation List and makes it available for download to certificate holders.[465]

2.13.4 Summary

Table 50 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 50: Summary and rating, Ireland, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2000. public accreditation and certification scheme for organizations	A
technical standard	eGovernment, eTax, other eServices all types of electronic signatures all types of certificates public accreditation and certification scheme 2 CSP CRL	A
distribution	On the eGovernment sit of reachservices.ie (requiring simple signature), about 100.000 users are registered currently. 65% of income tax returns were effected via ROS, requiring on qualified electronic signatures that are explicitly issued for this system. In 2005, about 93% of customs tax declarations are submitted via the new system ROS. There could no statistic be found on the actual use of qualified signatures or issued certificates or smartcards.	-

[465] cf. http://www.post.trust.ie/reposit/CRL.html, access on 28.07.07, 15:25

2.14 Italy

Figure 52: Fact-sheet: Italy, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 52 some basic demographic and geographic data of the country is presented.

2.14.1 Institutional frame

Legislation

Italy was a pioneer in the field of electronic signatures, being one of the first countries to give full legal value to electronically signed documents.

The first regulation on electronic signature was the DPR 513 of 1997, adopted in execution of article 15 of the Law n.59 of 15. March 1997. Subsequently, such regulation has been transposed in the DPR n. 445/2000 (Unified Body of Laws on the administrative documentation), modified and updated in the following years.

The European directive 199/93/CE was adopted with the D.lgs n. 10/02 and DPR April 2003 n.137.[466]

[466] cf. Correspondence with Antonio Cappiello, National Board of Italian Civil Law Notaries, Italy

With the legislative decree No. 82 of the 7th March 2005, named „Digital Administration Code“, the basics of digital technologies were constituted in public administration. After this decree, already existing e-Government services were developed also for provinces and municipalities.[467]

Other norms for digitalization of public administration have been dismissed:[468]
- Legal validity of digital documents and digital Signature, Ordinance of CNIPA, No. 4, 17.2.2005 (see Appendix - Italy: DELIBERAZIONE 17 febbraio 2005, Regole per il riconoscimento e la verifica del documento informatico).
- certified e-Mails: decree of the President, No. 68, 11.2.2005 (see Appendix - Italy: Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.).

Electronic documents with digital signatures based on a qualified certificate that are created with an secure signature creation device are legally binding and equivalent to handwritten signature.
Italy was one of the first countries in the European Union to grant full legal validity to digital signatures.[469]

•recognition of foreign certificates:[470]
In March 1998, the agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:
Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

---

[467] cf. Correspondance with Dr. Anna Maierhofer, for the commercial attaché for Italy, Federal Economic Chamber foreign trade office Padua

[468] cf. Correspondance with Dr. Anna Maierhofer, for the commercial attaché for Italy, Federal Economic Chamber foreign trade office Padua

[469] cf. Study of the Donau University Krems, Master-Study, Italy

[470] cf. Study of the Donau Universität Krems, Master-Studie, Austria

Availability of Online Services

•eGovernment:

The Ministry of Innovation has issued a „Guideline for Advancement of e-Democracy in Italy (only available in Italian (see Appendix - Italy: DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI, tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).[471]

Within the scope of a strategy plan of the European Commission eEurope2010[472], the Italian administration has launched 134 Projects in the area of eGovernment. The subjects concern amongst others the construction of portals and services for Businesses. Up to the present, nearly all projects have been completed.[473]

•Uniwex - eEducation:[474]

Uniwex is a system that allows professors of the University of Bologna to manage their documents and exams via the Website https://uniwex.unibo.it. Documents can be digitally signed with qualified signatures using a smart card and a simple web-based applications software.
About 1.000 persons use a digital signature and per year about 100.000 signatures are performed.

•Unimoney:[475]

To exchange financial documents between local government and banks, the unimoney system (www.unimoney.it) was developed. Documents that are transmitted via this system can be signed electronically with qualified signature. To make use of this application, a smart card is required. More than 20 institutions in Italy use this system and more than 300.000 documents are signed electronically each year.

•Telemaco - electronic filling system for business entities:[476]

All Italian enterprises must fill a Business Register with their data , like registration, amendment or closure notifications. The system Telemaco was implemented by Infocamere to simplify those procedures via the Web and made electronic filling with Chambers possible. The filing requires a qualified signature on smart cards. In 2005, 850.000 balance sheets have been submitted signed electronically to the Chambers of Commerce, and 4 millions documents relating to the Balance sheets have been signed electronically.

---

[471] cf. Correspondance with Dr. Anna Maierhofer, for the commercial attaché for Italy, Federal Economic Chamber foreign trade office Padua

[472] for more information see http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm

[473] cf. Correspondance with Dr. Anna Maierhofer, for the commercial attaché for Italy, Federal Economic Chamber foreign trade office Padua

[474] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Italy, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[475] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Italy, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[476] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Italy, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•PCCT - Online Civil Trial:[477]
The project PCCT was developed by the Ministry of Justice and is one of the most important eGovernment initiatives. PCCT was implemented to increase the availability of online services within a high-security PKI architecture and newest technical standards and is accessible under http://www.processotelematico.giustizia.it. The system provides strong authentication via smart cards and requires a qualified electronic signature. Currently about 300 internal and external users use eSignature in 7 sites among the system.

•Intercent-ER - eProcurement:[478]
Intercent-ER is an electronic procurement system that serves as an instrument for the Public Administration, purchasing goods and services from different businesses. Qualified signature is used to purchase in an eMarketplace, issue selling proposals and bid electronically. For other services the use of qualified signature is only mandatory. All in all, 116 administrations enrolled in this service (out of 647), thereof 54 Administration use qualified signature.
Form 2248 purchases, 668 are provided with a qualified electronic signature.

•Project CRS-SISS - eHealth:[479]
CRS-SISS is a Healthcare-Extranet that links social services, organizations, operations and citizens, providing events, information about patient treatment and value added services.
The project involves 9.200.000C citizens, 2.500 pharmacies, 49 Public Healthcare service Suppliers, and more.
Personal smart cards grant access to the Extranet. Advanced electronic signatures are mandatory for prescriptions, referrals and financial accounting files.
Currently approximately 3.450.000 prescriptions are logged per month, all digitally signed. About 140.000 referrals are digitally signed.

Types of electronic signature

The legislative decree 7 March 2005, n.82, defines three basic concepts of electronic signature:

- "electronic signature": is any system of electronic data association used in order to authenticate an electronic document
- "Qualified electronic signature": is an electronic signature based on a technology allowing the univocal identification of the signer, through a secure system associated only to him, and under his exclusive control, and whose electronic certificate is guaranteed from a third party (qualified certificate)

[477] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Italy, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[478] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Italy, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[479] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Italy, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

- „digital signature": is a particular type of "qualified electronic signature", built on cryptographic technology based on asymmetric keys.[480]

These types are responding to the same requirements as in the directive. In addition, the fourth type of electronic signature is the qualified electronic signature that has recognition of a higher level of signature. This is an advanced electronic signature based on a qualified certificate and created by a secure signature creation device.[481]

An electronic document signed with a qualified electronic signature has the same legal value of a hand signed paper document.[482]

Digital Signature is often used in public online advertisements. The PDF document is provided with a digital signature and loaded up.
In the year 2005, about 35 million documents with digital signature have been transmitted.[483]

2.14.2 Application requirements

Types of certificates
Actalis offers certificates for

- qualified digital signatures
- „light“ digital signature,
- code signing,
- strong online authentication (SSL/TLS client)
- secure websites (SSL/TLS server)
- secure e-mail (S/MIME)
- Windows smart card logon
- Virtual Private Networks (es. IPSEC)
- application-to-application (e.g., XMLDSIG)
- signing and/or encryption with hardware security modules (HSM)
- IC card terminal authentication (e.g., FINREAD)
- EMV (Europay/Mastercard/Visa)

[480] cf. Correspondence with Antonio Cappiello, National Board of Italian Civil Law Notaries, Italy

[481] cf. Study of the Donau Universität Krems, Master-Studie, Italy

[482] cf. Correspondence with Antonio Cappiello, National Board of Italian Civil Law Notaries, Italy

[483] cf. Correspondance with Dr. Anna Maierhofer, for the commercial attaché for Italy, Federal Economic Chamber foreign trade office Padua

On request, Actalis also offers Certificates with custom profiles.
These certificates can be used for any kind of device and for any application.
Actalis also offers a digital time-stamping service.

Certification Service Providers

➡Short description: Actalis[484]

Actalis offers certification services, PKI-enabling products as well as a range of professional services (like consultancy and training operations).
Actalis is an accredited certification service provider and issues and manages certificates for qualified digital signatures.

The other certification service providers are listed up in table 51.

Table 51: Certification Service Provider in Italy, source: own illustration

Certification Service Provider		Issued Certificates
Actalis		certificates for - qualified digital signatures - „light“ digital signature, - code signing, - strong online authentication (SSL/TLS client) - secure websites (SSL/TLS server) - secure e-mail (S/MIME) - Windows smart card logon - Virtual Private Networks (es. IPSEC) - application-to-application (e.g., XMLDSIG) - signing and/or encryption with hardware security modules (HSM) - IC card terminal authentication (e.g., FINREAD) - EMV (Europay/Mastercard/Visa) Certificates with custom profiles, on request digital time-stamping
Infocamere SC.p.A.		n.a.
Postecom		n.a.
Intesa		n.a.
Trust Italy		n.a.
Cedacri		n.a.
I.T. Telecom Italia		n.a.
Commando Transmissions and Information Army		n.a.
National council Forense		n.a.
SOGEI		n.a.

[484] cf. http://www.actalis.it/en, access on 03.12.2007, 18:54

Certification Service Provider		Issued Certificates
Sanpaolo	SANPAOLO	n.a.
Bank Mount of the Paschi of Siena	MONTE DEI PASCHI DI SIENA	n.a.
Integrated Lombardy	Lombardia Integrata s.p.a.	n.a.
Bank Understanding		n.a.
Bank of Rome	UniCredit Banca di Roma	n.a.
CNIPA	CNIPA	n.a.
Certicomm	certicomm	n.a.
Defense General Staff	MINISTERO DELLA DIFESA	n.a.

Inspecting authorities

The Centro Nazionale per Informatica nella Pubblica Amministrazione (CNIPA) is the Regulation Authority for digital signatures in Italy. It underlies the Italian Council of Ministers and has authority in the areas e-Gov, public ICT services, IT-security and innovations of ICT. Certification Service Providers must be accredited by the CNIPA.[485]

2.14.3 Technical preconditions

Signature Software

Digital Signature is often used for public online announcements. Therefore the pdf document is provided with a digital signature and loaded up. The autonomous region Friaul Julisch-Venetien is very progressive in the area of e-procurement and e-government and uses p7m programm that is free for download under: http://acquisti.regione.fvg.it/portal/page?_pageid=35,50324&_dad=portal&_schema=PORTAL .[486]

Types of secure signature-creation device

Italy is the european country with the highest rates on issued smart cards: 2,6 million 75% of the smart cards with digital signature are issued to businesses, the remaining to freelancers and employees of the public administration.[487]

Card readers

n.a.

[485] cf. Correspondance with Dr. Anna Maierhofer, for the commercial attaché for Italy, Federal Economic Chamber foreign trade office Padua

[486] cf. Correspondance with Dr. Anna Maierhofer, for the commercial attaché for Italy, Federal Economic Chamber foreign trade office Padua

[487] cf. Correspondance with Dr. Anna Maierhofer, for the commercial attaché for Italy, Federal Economic Chamber foreign trade office Padua

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

2.14.4 Summary

Table 52 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 52: Summary and rating, Italy, source: own illustration

categories		rating
legal framework	Italy was a pioneer in the field of electronic signatures and was one of the first countries to give full legal value to electronically signed documents. The firs regulation on electronic signature was adopted in 1997. The EU directive was adopted in 2002.	A
technical standard	eGov, eTax, eHealt, eProcurement, eEducation all types of electronic signatures all types of certificates a huge range of certification service providers	A
distribution	Digital signature is often used in public online advertisement. In 2005 about 35 million documents with digital signature have been transmitted. Italy is one of the countries with the highest rates on issued smart cards: 2.6 million smart cards, thereof 75% were issued to businesses. In the area of eEducation About 1.000 persons use a digital signature and per year about 100.000 signatures are performed. More than 20 institutions in Italy use the system Unimoney for exchanging data and more than 300.000 documents are signed electronically each year. In 2005, 850.000 balance sheets have been submitted signed electronically to the Chambers of Commerce via Telemaco, and 4 millions documents relating to the Balance sheets have been signed electronically. Currently about 300 internal and external users use eSignature in 7 sites among the system PCCT. Concerning Intercent-ER, 116 administrations enrolled in this service (out of 647), thereof 54 Administration use qualified signature. Form 2248 purchases, 668 are provided with a qualified electronic signature.	A

2.15 Latvia

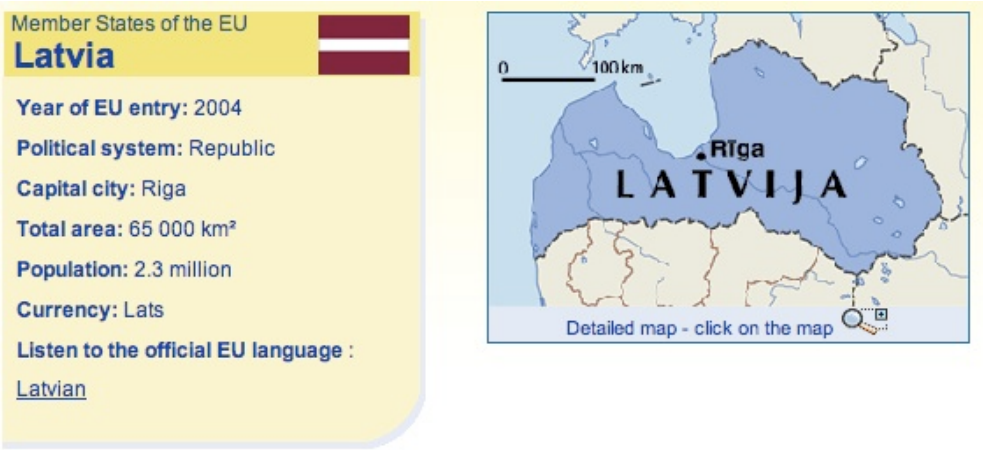


Figure 53: Fact-sheet: Latvia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:51

In figure 53 some basic demographic and geographic data of the country is presented.

2.15.1 Institutional frame

Legislation

In October 2002, the Law on Electronic Documents (see Appendix – Latvia: Electronic Documents Law) was adopted by the Latvian Parliament. It defined the legal status of e-documents and e-signatures.[488]

This law was implemented in Latvian Republic and came into force at 1 January 2003.[489]

In September 2006, the first trusted certification service provider was established. Since then, all state institutions must accept electronic documents that are signed with qualified electronic signatures.[490]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Latvia: National Regulations Details.[491]

---

[488] cf. http://ec.europa.eu/idabc/en/document/5923, access on 15.06.2007, 18:09

[489]cf. Correspondence with Iveta Smite, Latvian Post, Latvia

[490] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Latvia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[491] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Availability of Online Services

•eGovernment

Latvia is anxious to establish an eGovernment, but has to face some barriers:[492]

- little penetration of Internet because of high access costs (table 53)
- absence of fix telephone lines in most rural regions
- absence of electronic signatures
- no public know access-point, that lists up the existing public online-services and information about that.

Table 53: Information Society Indicators 2005, source: http://www.euser-eu.org/eUSER_eGovernmentCountryBrief.asp?CaseID=2208&CaseTitleID=1032, access on 15.06.2007, 18:02

	Latvia	Average in Europe
Internet penetration	15%	42%
Broadband penetration	1.5%	6.5%
ICT expenditure	7.3%	2.6%

In the last years, the expenses in the range of Information and Communication Technology (ICT) have been increased (see table 53), both in the public sector and at the private companies. Furthermore, an Information society has developed and three governmental projects were implemented (Unified Information System of Municipalities, National Unified Library Information System, Education Information System). These Facts of course supply the establishment of an e-Government.

The use of electronic signature in eGovernment applications is very limited.[493]

•eTax:

The only eGovernment application that is using electronic Signature is the eTaxing System - the Electronic Declaration System established by the State Revenue Service. Currently, about 95% of all reports and tax declarations can be submitted electronically to the State Revenue Service, either via the website or by sending prepared files. Additionally, all documents had to be sent in paper as well. The Electronic Declaration System was set um in 2001. In March 2006, an instruction was adopted, the „Agreement on signing electronic documents with the electronic signature using the State Revenue Service electronic declaration system services, and ensuring these services“. According to that agreement , all users that conclude it, do not need to submit their reports in paper format anymore. The User is provided with all necessary data for creation a signature (password and software) and thus the data can be verified by the State Revenue Service.[494]

---

[492] cf. http://www.euser-eu.org/ShowCase.asp?CaseTitleID=549&CaseID=1265&MenuID=109, access on 15.06.07, 18:07

[493] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Latvia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[494] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Latvia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

No statistics could be found on the actual use of electronic signatures but the number of users that use eTax applications is increasing.[495]

Types of electronic signature

The electronic signature was implemented by the end of September 2006[496] by the Latvian Post CSP.[497]

Current implementation of electronic signature, assume usage of qualified certificates for the non-repudiation, thus we are talking about secure electronic signature.[498]

Qualified signatures are not used yet in practice in eProcurement.[499]

The electronic signature is free for all employees of the governmental administration departments.[500]

- eSignature Card:

The Cabinet of Ministers adopted a Regulation on the citizens' identity cards that provides the integration of electronic chips in the identity cards. That chip should contain the holders name and sex, a digital picture, a personal identity number as well as an e-signature.[501]

The Latvian government strives forward to implement a digital e-signature infrastructure. Microsoft Services shall provide the Latvian Post with a solution called Microsof.NET Framework and Windows Server 2003. Since October 2006, citizens, businesses and civil servants can use smartcards to access all government and also commercial electronic services. New transactional e-government services are added to the infrastructure, including education and healthcare. Some of he Benefit of this project is, that the solution is compliant with the EU standards and new e-services can be added. The solution is going to be extended also for non-Microsoft systems.

According to this solution, the user receives a smart card with two types of certificates, one for creating a qualified digital signature and another one for authentication. With this card, citizens can be identified and authenticated when they access an online public service. Also civil servants become identified when they log in departmental applications.

The card also enables to add a digital signature to documents and data and lock the document.

---

[495] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Latvia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[496] cf. Correspondence with Herwig Palfinger, head of the branch office in Riga, Austrian Federal Economic Chamber

[497] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

[498] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

[499] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Latvia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[500] cf. Correspondence with Herwig Palfinger, head of the branch office in Riga, Austrian Federal Economic Chamber

[501] cf. http://www.epractice.eu/index.php?page=document&doc_id=3404&doclng=6, access on 15.06.2007, 19:36

In October 2006, the Latvian Post issues the first certified eSignature card that enables to electronically sign documents and access to on-line eServices.

In February 2007, Electronic Signature is made available for the customers of Hansabanka-Swedbank. Customers have the opportunity to authenticate themselves for the e-banking service by using the e-signature card, both private customers (Hanza.net) and business customers (Telehansa.net).[502]

2.15.2 Application requirements

Types of certificates

Smart card media is used to implemented electronic signature. Qualified certificates are provided for the electronic document signing. Also time stamp technology is in place for the secure control of time stamps for electronically signed documents. Pin code is used to secure the operations with electronic signature smart card.

Software certificate services are under development process.[503]

Certification Service Providers

Only one CSP is working in the Latvian Republic. In 2006, the first trusted certification service Provider, the JSC Latvian Post, has been accredited by the Data State Inspection.[504]

➡Short description: JSC Latvian Post[505]

JSC Latvian Post (Latvijas Pasts) - The basic activity of the state-owned JSC Latvian Post is rendering mail services to private individuals and legal entities of the Republic of Latvia.

➡Short description: E-ME

It is the CSP division of JSC “Latvian Post” that provide certification services to natural persons, government and business entities in Latvian Republic. Full portfolio of certification related services are provided: several packages of electronic signature (oriented on natural persons, small and medium enterprises and large enterprises), control of certificates and online checking, revocation lists, OCSP, dynamic requests, etc.

JSC Latvian Post is constantly works on new products and services to extend abilities of our customers.

---

[502] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

[503] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

[504] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

[505] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

Table 54 lists up all certification service providers in Latvia.

Table 54: Certification Service Provider in Latvia, source: own illustration

Country	Certification Service Provider	Issued Certificates
Latvia	JSC Latvian Post	qualified certificates

Inspecting authorities

The Data State Inspection is the organization that supervises personal data protection in Latvian Republic.[506]

2.15.3 Technical preconditions

Signature Software

Special software (eSigner) for creation, signing, time stamping and checking is available at E-ME website at no cost for all customers. Software is working in the Microsoft Windows environment. Special applet is also available for Windows and other operating systems to perform the same functionality from the Java-enabled browser.[507]

The Software can be downloaded on http://info.e-me.lv/en/atbalsts/programmatura/eParakstitajs.html.

Types of secure signature-creation device

•eSignature Card

The Latvian Post provides special smart cards (E-ME cards) for electronic signature.[508]

On the homepage of EME drivers for the use of the eSignature smart Card can be downloaded: http://info.e-me.lv/en/atbalsts/programmatura/driveri.html.

Card readers

The Latvian Post supports several card readers and keyboards (table 55 and 56). Readers with PIN-pads are recommended for environments with no sufficient control.[509]

[506] cf. http://www.dvi.gov.lv/eng, access on 30.07.07, 16:16

[507] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

[508] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

[509] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

Table 55: Smartcard reader recommended by the Latvian Post, source: http://info.e-me.lv/en/atbalsts/lasitaji.html, access on 30.07.2007, 16:19

provider	Smartcard reader		connection	Operating System
Gemplus, http://www.gemplus.com	GemPC Twin		USB	Win 98, 98SE, Me, 2000, XP Linux, MacOS X upon request
scm microsystems, http://www.scmmicrol.com	SCR3310		USB	Windows 98, ME, 2000, XP, Server2003, Windows CE 4.2, 5.0 MacOS, Linux, Solaris
scm microsystems, http://www.scmmicrol.com	SCR243		PC Card	Windows 98, ME, NT4, 2000, XP, Server2003, Windows CE 4.2, 5.0 MacOS, Linux
Gemplus, http://www.gemplus.com	GemPC Card		PC Card	Win 98, 98SE, Me, NT4, 2000, XP, Server2003, Xp 64bit, Server 2003 64bit, Linux

Table 56: Supported Card Readers included in Keyboards, source:http://info.e-me.lv/en/atbalsts/lasitaji.html, access on 30.07.2007, 16:19

provider	Keyboard		Operating System
Cherry	SmartBoard G83-6744		Windows 98, ME, 2000, XP, Xp 64bit, CE MacOS, Linux
Cherry	SmartBoard G83-6644		Windows 98, ME, 2000, XP, Xp 64bit, CE MacOS, Linux, Vista
Cherry	SmartBoard G83-6733		Windows 98, ME, 2000, XP, Xp 64bit, CE MacOS, Linux

Certificate requirements

n.a.

Application programming interface for online-verification

API for online verification is available; also there is ability to check signatures online on the CSP website.[510]

[510] cf. Correspondence with Iveta Smite, Latvian Post, Latvia

o verify electronically signed document or electronic signatures, no eSignature smart card is needed, only the EME offered software must be installed.

The verification service, supplied by EME is accessible for anyone. It is free of charge and accessible in different formats:

- CRL records,
- LDAP catalogue and
- OCSP replies service formats[511]

2.15.4 Summary

Table 57 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 57: Summary and rating, Latvia, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2003. Furher regulation on citizens identity card (eSignature card).	A
technical standard	eGov, eTax eGov implementation faced some barrieres (little internet penetration, absence of eS) Electronic signature implemented in 2006, since Oktober 2006, smartcards to access eGovernment and other eServices smartcards containing 2 certificates (qualified C, and authentication) SW certificates under development several card readers CRL, LDAP, OCSP	B
distribution	Little internet penetration, absence of electronic signature eGov: use of eS in eGov applications is very limited. eTax: no statistics on use of eS, but the number of eTax users is increasing. eProcurement: no practical se of qualified signatures Since Feb 2007, ES available for customers of Hansabanka-Swedbank for e-banking services.	C

[511] cf. http://info.e-me.lv/en, access on 15.06.07, 19:42

2.16 Lithuania

Figure 54: Fact-sheet: Lithuania, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:52

In figure 54 some basic demographic and geographic data of the country is presented.

2.16.1 Institutional frame

Legislation

The EU-directive was implemented in the national law via the Law for electronic Signature Nr. VIII-1822 on the 11.07.2000 (see Appendix – Lithuania: Law on Electronic Signature).

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Lithuania: National Regulations Details.[512]

Availability of Online Services

•eGovernment:

In Lithuania, the importance of eGovernment increases from year to year. There is a common portal (http://www.govonline.lt), where some basic administration services are supplied online. But to use these applications completely, the implementation of digital Signature is lacking.[513] None of the eGov applications are using electronic signature to sign specific transactions.

[512] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[513] cf. Correspondence with Herwig Palfinger, head of the branch office in Riga, Austrian Federal Economic Chamber

The eGovernment portal aims to establish one point of access for all eGovernment services.[514] The main page of the portal is shown in figure 55.

Figure 55: eGovernment portal, Lithuania, source: http://www.govonline.lt, access on 05.09.2007, 18:27

In 2004, the Information Society Development Committee started to provide certification services to institution that participate in a pilot project „Installation of eSignature in State Institutions“. This project aims at facilitation of interchange of electronic documents between state institutions. But the committee does not provide qualified certification services.
Starting in 2005, the Committee implemented the „eSignature Infrastructure Development Project“ to implement devices for eSignature creation and verification in all state institutions. Thus, public servants are able to sign documents electronically and use eSignature when providing electronic Government services. The new eSignature software program „Justa GE“ was introduced recently (see chapter Technical preconditions - signature software: Justa GE)

On 2 June 2006, the Internet Portal paslaugos.evaldzia was launched as part of the project „Government electronic gates“ (figure 56). Users gain access to eGovernment services offered by various institutions using uniform identification means: eBanking identification or personal digital certificates. The data are held by UAB „Skaitmeninio sertifikavimo centras“ or by the bank and used for authentication. The portal offers the possibility to check paid taxes by the employer, medical services rendered and prescribed medicaments.[515]

[514] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Lithuania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[515] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Lithuania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

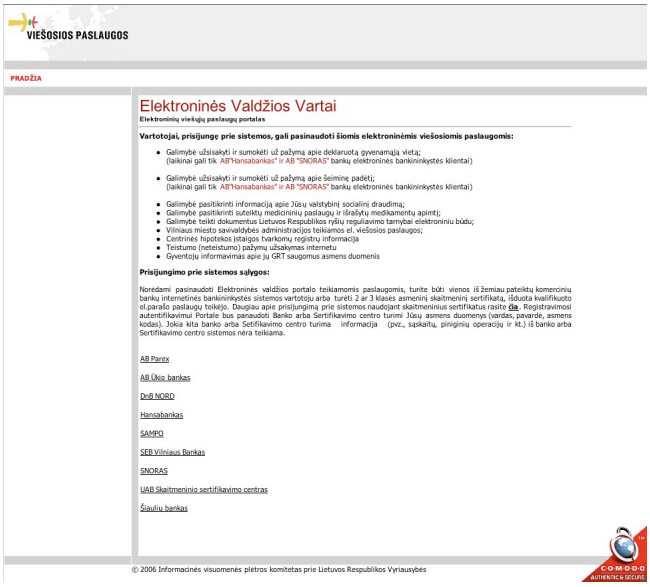


Figure 56: Internet portal of eGovernment services paslaugos.evaldzia.lt, source: https://paslaugos.evaldzia.lt/, access on 28.11.2007, 11:14

•eTax:[516]

In March 2004, an Electronic Tax Declaration System was launched. Individuals and legal entities can submit their tax reports electronically. The interaction between user and public service providers is completely electronically. The authentication of the persons relies on an agreement with the State Tax Inspectorate.

The Electronic Tax Declaration System currently does not use electronic signatures.

•EDAS:[517]

This system started from beginning of this year and was developed for signing electronic declarations in the State social ensurance agency. There are no statistics about the use of electronic signatures yet.

•other eServices:[518]

All operational and planned eGovernment applications are listed up in the Appendix - Lithuania: Operational and planned applications.

[516] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Lithuania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[517] cf. Correspondence with Evaldas Zidonis, Head of Electronic signature supervision devision, ISDC under Government, Lithuania

[518] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Lithuania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Types of electronic signature

Pilot projects concerning eSignature are under construction since a few years and are applied by some governmental institutions.

The „Pilot Project of Electronic Signature Implementation in the Public Institutions“ was launched in 2003. Its target was to boost the e-government progress in Lithuania by enabling secure electronic exchange of documents between public administration institutes.[519]

The Digital Certification Center Skaitmeninio Sertifikavimo Centras (SSC) is responsible for the implementation and distribution of digital signature.

For a fast implementation of the eSignature project a coordination committee of the Lithuanian government was founded (http://www.signature.lt). Members are representatives of four important Business banks as well as of two telecommunication companies. [520]

In the fist project stage in May 2004, five public institutions have started to exchange documents electronically with using electronic signatures. In the second stage in December 2004, the system was expanded to twenty public institutions. The participating institutions received special chip cards, which contained certificates and private and public keys. For using these chip cards, free signature-authentication software had to be installed. The target of this project was to enable all public institutions to change their documents electronically.[521]

In February this year, a uniform standard for e-Signature should have been designed, but has not been affected to date. By 2009, about 300.000 eSignatures shall be distributed to natural persons.[522]

The people that hold such certificate can use their eSignature to get access to different eServices.

Members of this eSignature Initiation program are SODRA, PAREX Bank and DNB Nord Bank.[523]

The business Banks plan to implement an e-Banking system. It already exists, but on a low level that is not conform to the standards of digital signature. [524]

Actually, in closed user groups, there are used basic and secure electronic signatures. In open systems commonly advanced signature is used.

There are some solutions concerning the format of the signatures. Often CMS format is used., for governmental institution there is recommendation to use XAdES-BES and higher - today in fact till -C

---

[519] cf. http://ec.europa.eu/idabc/en/document/3697/590, access on 26.06.07, 18:08

[520] cf. Correspondence with Herwig Palfinger, head of the branch office in Riga, Austrian Federal Economic Chamber

[521] cf. http://ec.europa.eu, access on 15.06.07, 20:00

[522] cf. Correspondence with Herwig Palfinger, head of the branch office in Riga, Austrian Federal Economic Chamber

[523] cf. http://www.dmeurope.com, access on 26.06.2007, 18:12

[524] cf. Correspondence with Herwig Palfinger, head of the branch office in Riga, Austrian Federal Economic Chamber

(there is offered free signature creation an verification s/w for XAdES formats on http://epp.ivpk.lt/epp/download/Justa_GE_v1.0.30RC7.zip).[525]

In 2005, a project, eSignature Initiation Program (E3P), was initiated by mobile telecommunication companies, planning to place electronic signature data and qualified certificates into SIM card of mobile phones. In this project users are recommended to start from XAdES - EPES.[526]
Lithuanian Telco Omnitel has developed a service that enable creation a digital signature with using their handsets. The SIM card enables to generate the digital signature, the mobile phone replaces the card reader.

The Lithuanian Parliament's Committee on the Development and Information Society started to use those mobile digital signatures internally. Lithuania was so one of the fist who implemented such an infrastructure worldwide.[527]

Electronic signature is used for some eServices, like for EDAS system and some eBanking systems already started to use electronic signatures. But mostly, instead of electronic signatures, it is still more popular to use the eBanking systems for authentication.
The eService Portal uses electronic signatures only for authentication.
Though 90% of tax and property declarations were provided in electronic form, the only possibility to use electronic signature was for authentication.[528]

2.16.2 Application requirements

Types of certificates

The government coordination committee agreed starting the distribution of eSignature certificates to citizens. The plan was to issue 300.000 certificates until 2009. With such certificates, people have the possibility to use eSignature to access new eServices that are specially developed.[529]

In Lithuania, only qualified certificates can be obligatory registered. Basic requirements are available in „Requirements for Providers of Certification Services, creating Qualified Certificates, Requirements for Electronic Signature equipment, Procedure of registration of Providers of Certification Services, creating Qualified Certificates and control and Confirmation of regulations of Electronic Signature Supervision" (see Appendix - Lithuania, Requirements for Providers of Certification Services, creating Qualified Certificates, Requirements for Electronic Signature equipment, Procedure of registration of Providers of Certification

[525] cf. Correspondence with Kristina Aidietiene, Specialist of the Information and EU issues Division, Information Society Development Committee, under the government of the Republic of Lithuania

[526] cf. Correspondence with Kristina Aidietiene, Specialist of the Information and EU issues Division, Information Society Development Committee, under the government of the Republic of Lithuania

[527] cf. http://www.dmeurope.com/default.asp?ArticleID=6086, access on 26.06.2007, 18:10

[528] cf. Correspondence with Evaldas Zidonis, Head of Electronic signature supervision devision, ISDC under Government, Lithuania

[529] cf. http://ec.europa.eu/idabc/en/document/6574/194, access on 26.06.07, 17:39

Services, creating Qualified Certificates and control and Confirmation of regulations of Electronic Signature Supervision).
Qualified certificates are issued by UAB „Skaitmeninio Sertifikavimo Centras“. Technical specifications of the certificates issued by UAB are listed in Appendix - Lithuania: Technical specifications of the certificates issued by UAB „Skaitmeninio Sertifikavimo Centras“.

There is a possibility to obtain basic software and hardware qualified certificates.[530]

According to IVPK, only some thousands of PKI certificates are in operation today: about 2.000 qualified certificates, 6.000 non qualified certificates and about 5.000 software certificates of them.[531]

Certification Service Providers

Currently, only one Certification Service Provider issues qualified certificates in Lithuania - UAB “ Skaitmeninio Sertifikavimo Centras“.[532] The Digital Certification Centre Skaitmeninio Sertifikavimo Centras (SSC) is also responsible for the implementation and distribution of digital signature.

➡Short description: Skaitmeninio Sertifikavimo Centras[533]
SSC is privately owned and was established in 2004. It is a leading Internet security provider, offering E-commerce Security Solutions, Certificate services, Crypto Solutions, Validation Services and software security applications.
SSC was incorporated in 2004 as a private company. Early 2005 officially recognized by Government as a Qualified Certification Authority. The company focuses in both the certification and consulting services. Active in e-government and e-business markets. The Root Certificate of the company is listed in Microsoft's Trusted Root Certification Authority list. By the end of year the Root Certificate will also be included in FireFox and Opera trusted Root lists.
SSC offers a complete set of certification services (from issuing to revocation) for citizens, Code signers and site owners.[534]

Ttable 58 lists up all certification service providers in Lithuania.

Table 58: Certification Service Provider in Lithuania, source: own illustration

Certification Service Provider		Issued Certificates
Skaitmeninio Sertifikavimo Centras	SKAITMENINIO SERTIFIKAVIMO CENTRAS	qualified certificates

[530] cf. Correspondence with Kristina Aidietiene, Specialist of the Information and EU issues Division, Information Society Development Committee, under the government of the Republic of Lithuania

[531] cf. Correspondence with Evaldas Zidonis, Head of Electronic signature supervision devision, ISDC under Government, Lithuania

[532] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Lithuania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[533] cf. http://www.scs.lt/?name=menu&act=show&do=13&L=en, access on 06.08.07, 22:35

[534] cf. Correspondence with CEO, Skaitmeninio Sertifikavimo Centras, Lithuania

There are Certification Service Provider, which provide services for local closed system (e.g., providing certificates for public servants for signing documents or in Lithuanian bank for other banks for internet banking payment systems).[535]

There are also foreign Qualified Certification Service Provider trying to provide their services through local mediators or directly, for example Estonian AS „Serfifitseerimiskeskus“ or the Polish „CERTUM“.[536]

Inspecting authorities

For the coordination of all IT-project (eGovernment, eMunicipality, digital Signature etc.) the Information Society Development Committee under the Government of the Republic of Lithuania is responsible.[537]

This exercising authority is carrying out the functions of an institution of electronic signature supervision.[538]

The regulation authority for telecommunication services is called Rysiu reguliavimo tarnyba (RRT) that coordinates all issues concerning electronic communications.

2.16.3 Technical preconditions

Signature Software

Software development and support is offered by Elektroniniai verslo projektai (http://www.evp.lt). Natural and legal persons introduced to the e System via the homepage http://www.eparasas.lt.

The information Society Development Committee was assigned with the implementation of the project and chooses E-Lock ProSigner as digital signature software. E-Lock ProSigner is a desktop digital signature software, developed by Frontier Technologies. This software can be integrated in MS Word, Excel, Adobe Acrobat and the Windows environment.[539]

➡Short description: Frontier Technologies[540]

Frontier Technologies is a privately owned corporation in the US. By launching a range of digital signature products, E-Lock entered the market for PKI and Security in 1997.

---

[535] cf. Correspondence with Evaldas Zidonis, Head of Electronic signature supervision devision, ISDC under Government, Lithuania

[536] cf. Correspondence with Evaldas Zidonis, Head of Electronic signature supervision devision, ISDC under Government, Lithuania

[537] cf. Correspondence with Herwig Palfinger, head of the branch office in Riga, Austrian Federal Economic Chamber

[538] cf. Correspondence with Kristina Aidietiene, Specialist of the Information and EU issues Division, Information Society Development Committee, under the government of the Republic of Lithuania

[539] cf. http://ec.europa.eu/idabc/en/document/3697/590, access on 26.06.07, 18:08

[540] cf. http://www.elock.com, access on 26.06.2007, 19:29

•Justa GE

Two years ago UAB „Skaitmeninio sertifikavimo centras“ created a document signing software known as Justa GE. The software can sign any documents, files etc. Supports XAdES standard (currently up to C format). The software is distributed free of charge and runs under Windows (almost all flavors) and Linux (depends on availability of smart card and eToken drivers).[541]

The use of eSignatures is not widespread in practice.[542]

Types of secure signature-creation device

secure eTokens, smart cards and SIM cards[543]

Some mobile operators (together with banks and the support of Government formated public partnership programmes for stimulation of the use of electronic signatures) have started to propose SIM cards with electronic signature keys and certificates.[544]

For the participant institutions of the pilot-project on the implementation of electronic signature, special chip cards were distributed. These chip cards include certificates and a public and private key to give the possibility of exchanging documents electronically.

The service, launched by the Lithuanian Telco Omnitel, allows the use of mobile phones for creating digital signatures. The signature is generated by the mobile SIM card, the mobile phone replaces the card reader.[545]

Card readers

For smart cards SSC uses Gemalto readers. For PIN entry the signing software supports keyboard.

Certificate Requirements

In Lithuania, only qualified certificates can be obligatory registered. Basic requirements are available in „Requirements for Providers of Certification Services, creating Qualified Certificates, Requirements for Electronic Signature equipment, Procedure of registration of Providers of Certification Services, creating Qualified Certificates and control and Confirmation of regulations of Electronic Signature Supervision“ (see Appendix - Lithuania, Requirements for Providers of Certification Services, creating Qualified Certificates, Requirements for Electronic Signature equipment, Procedure of registration of Providers of Certification Services, creating Qualified Certificates and control and Confirmation of regulations of Electronic

---

[541] cf. Correspondence with CEO, Skaitmeninio Sertifikavimo Centras, Lithuania

[542] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Lithuania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[543] cf. Correspondence with CEO, Skaitmeninio Sertifikavimo Centras, Lithuania

[544] cf. Correspondence with Evaldas Zidonis, Head of Electronic signature supervision devision, ISDC under Government, Lithuania

[545] cf. http://www.dmeurope.com/default.asp?ArticleID=6086, access on 26.06.2007, 18:10

Signature Supervision).

For the chip cards, distributed for the implementation of electronic signature, a special Signature-authentication-software is necessary. This software is free available.[546]

Application programming interface for online-verification

The SSC offers an OCSP service on their homepage (http://ocsp.ssc.lt).[547]

2.16.4 Summary

Table 59 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 59: Summary and rating, Lithuania, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2000.	A
technical standard	eGovernment with some basic online administration services, but implementation of eS is lacking, none of eGov applications use eS 2003, Pilot project of Electronic Signature Implementation in the Public Institution, target was to enable public institutions to exchange documents electronically 2005, eSgnature Initiation Program for eS data and qualified certificates on mobile SIM cards. Lithuania was one of the first to implement mobile signature Infrastructure in Parliament, basic software and hardware qualified certificates chip cards, mobile SIM cards OCSP	B
distribution	eGovernment with some basic online administration services, but implementation of eS is lacking, none of eGov applications use eS, if eS is used, then only for authentication Programmes to stimulate the use of eS Start of distribution of eSignature certificates for citizens (plan: 300.000 until 2009) According to IVPK, only some thousands of PKI certificates are in operation today: about 2.000 qualified certificates, 6.000 non qualified certificates and about 5.000 software certificates of them	B

[546] cf. http://www.visualbuilder.com/viewnews.php?group_id=15&news_id=633, access on 26.06.2007, 19:39

[547] cf. Correspondence with CEO, Skaitmeninio Sertifikavimo Centras, Lithuania

2.17 Luxembourg

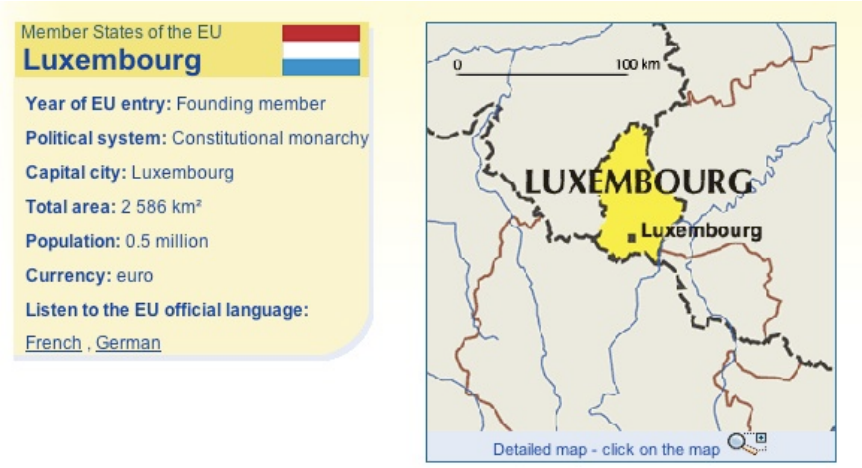


Figure 57: Fact-sheet: Luxembourg, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 57 some basic demographic and geographic data of the country is presented.

2.17.1 Institutional frame

Legislation

In Luxembourg, the Signature Directive 1999/93/CE was implemented in national law in the eCommerce Act of 14 August 2000 („Loi du 14 aout 2000“, see Appendix - Luxembourg: eCommerce Act (2000)) and is completed by the Regulation on Electronic Signatures and Electronic Payments of 1 June 2001 („Règlement granducal du 1er juin 2001 relatif aux signatures électroniques, au paiment et à la création du comité ‚commerce électronique‘, see Appendix - Regulation on Electronic Signatures and Electronic Payments (2001))“.[548]

Currently, there is no overall eGovernment legislation in Luxembourg.

All national regulations concerning eCommerce and electronic signatures can be found in detail in the Appendix - Luxembourg: National Regulations Details.[549]

[548] cf. Correspondance with Mag. Peter Fuchs, for the commercial attaché forBelgium and Luxembourg, Federal Economic Chamber foreign trade office Bruxelles

[549] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Availability of Online Services

•www.entreprises.public.lu - eBusiness Portal:

In November 2004, the government launched the Business portal (http://www.entreprises.public.lu/) for companies and entrepreneurs that delivers information and services, for example general business informations, advices for companies, downloadable forms etc.[550] The entry site of the portal is shown in figure 58.

Figure 58: Business Portal, source: http://www.entreprises.public.lu, access on 28.11.2007, 11:16

•eGovernment:

To accelerate the eGovernment progress Luxembourg presented a master plan in February 2005. The total e-Government plan is available for download under http://www.eluxembourg.public.lu/Focus_content/plan_directeur1/plan_directeur.pdf. The responsible authority for the eGovernment strategy is the Ministry of the Civil Service and Administrative Reform.[551]

eLuxembourg is the eGovernment Portal. The main page of the portal is shown in figure 59.

[550] cf. European Commission, eGovernment Factsheets, eGovernment in Luxembourg, February 2007

[551] cf. European Commission, eGovernment Factsheets, eGovernment in Luxembourg, February 2007

Figure 59: eLuxembourg, eGovernment Portal, source: http://www.eluxembourg.public.lu, access on 28.11.2007, 11:18

In March 2003, LuxTrust (Luxembourg national certification authority, see Certificaten Service Providers) charged the consortium u-trust (consisting of Cetrel, Clearstream, Hitec and eBRC) with the implementation of a Public Key Infrastructure[552] to secure eGovernment and eCommerce in Luxembourg.[553].

Currently, no eGovernment service uses electronic signature. Only electronic VAT declaration, the eTVA system, uses simple signature for authentication, only consisting of username/password.[554]

•eInvoices:
In Luxembourg, only 13 % of enterprises received their orders electronically, this is substandard in the European Union. [555]

[552] cf. Correspondance with Mag. Peter Fuchs, for the commercial attaché forBelgium and Luxembourg, Federal Economic Chamber foreign trade office Bruxelles

[553] cf. European Commission, eGovernment Factsheets, eGovernment in Luxembourg, February 2007

[554] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Luxembourg, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[555] cf. Holpert, Andreas, Eine Chipkare für die Sicherheit, Artikel im Luxemburger Wort, 10.01.2008

Types of electronic signature

Electronic Signatures can be classified into the following five categories:

- „simple electronic signature, without certificate;
- electronic signature with a non-qualified certificate provided by a non-accredited certification service provider;
- electronic signature with a non-qualified certificate provided by an accredited certification service provider;
- electronic signature with a qualified certificate provided by a non-accredited certification service provider; and
- electronic signature with a qualified certificate provided by an accredited certification service provider.“[556]

The last two types of electronic signatures are recognized as legally binding and equivalent to handwritten signature and must fulfill the following requirements:

- creation through a secure signature device,
- control over the device by the signing party,
- Securisation by a qualified certificate.[557]

2.17.2 Application requirements

Types of certificates

LuxTrust issues Certificates signing server, Certificates SSL and Trusted time stamping.

LuxTrust Signing Server Certificates ensures a high security standard in combination with a system to access applications easily in complete security.

The certificate is saved on a secured server by which the certificate and the private key can be accessed, either by the LuxTrust token (using access code and personal password) or by the SMS solution (a SMS is generated automatically and sent to mobile phone of the user each time he logs in, use of sms an personal password to access private key).[558]

Currently it is not intended that LuxTrust issues qualified certificates.

---

[556] cf. Le Goueff, Stéphan, Sotiri, Erwin, Getting the deal through: e-commerce, http://vocats.com/index.php?id=170, access on 28.11.2007, 11:19

[557] cf. Le Goueff, Stéphan, Sotiri, Erwin, Getting the deal through: e-commerce, http://vocats.com/index.php?id=170, access on 28.11.2007, 11:19

[558] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Luxembourg, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Certification Service Providers

LuxTrust S.A. was instituted by the government, large banks and different private institutes as Luxembourg national electronic certification authority.[559]

Table 60 lists up all certification service providers in Luxembourg.

Table 60: Certification Service Provider in Luxembourg, source: own illustration

Certification Service Provider		Issued Certificates
LuxTrust S.A.	LUXTRUST Home Recherche Links Sitemap	Certificats signing server Certificate SSL et Objet time stamping

Inspecting authorities

The Chamber de Commerce de Luxembourg is the Luxembourg registration authority.

The Office Luxembourgeois d'Accréditation et de Surveillance (Olas) is responsible for the accreditation of certification service providers.[560]

2.17.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

•eID infrastructure:

Currently there is no central eID infrastructure or plans for an establishment.[561]

•LuxTrust chip card:

LuxTrust, the Luxembourg certification service provider, ensures secure electronic data transmission and wants to issue electronic chip cards, with that electronic communication becomes easier. With this card, also applications can be used that require electronic signature. This offer is an important element of the eGovernment strategy of Luxembourg. Relationships and communication shall be ameliorated between government and citizens.

In the next weeks, civil servants will be equipped with those chip cards (figure 60). [562]

---

[559] cf. Correspondance with Mag. Peter Fuchs, for the commercial attaché forBelgium and Luxembourg, Federal Economic Chamber foreign trade office Bruxelles

[560] for more information see: http://www.olas.public.lu

[561] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Luxembourg, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[562] cf. Holpert, Andreas, Eine Chipkare für die Sicherheit, Artikel im Luxemburger Wort, 10.01.2008

Figure 60: LuxTrust chip card, source: https://www.luxtrust.lu/index.php?id=41#c59, access on 28.11.2007, 11:25

Card readers

LuxTrust recommends the following Card Readers (table 61):

Table 61: Available card readers in Luxembourg, source: https://www.luxtrust.lu/fileadmin/user_upload/downloads/LuxTrust_SC_reader_List.pdf, access on 28.11.2007, 11:25

type of card readers	mark (models)		connection
Gemalto	GemPC Twin, new name Safesite Twin USB Reader		USB
	GemPC USB-SL new name Safesite USB - SL Reader		
	GemPC Twin [Serial] new name Safesite Twin seriell Reader		serial
	USB Floppy Bay Pack 3” ½ for PC Twin reader new name: USB Floppy Bay Pack 3” ½ for PC Twin reader		
	Stand for PC Twin		
	GemPC Card new name: Safesite PCCard Reader		
	GemPC Card new name: Safesite Express Reader		

Further, Luxtrust reccommendes card readers offerd by the following providers, listed up in table 62:

Table 62: Provider of card readers, recommended by Luxtrust, source: own illustration

Recommended Providers of card readers		link
Linsys	LinSys	http://www.linsys.lu/
Conostix	CONOSTIX	http://www.conostix.lu/products/luxtrust-reader.html
Enterprise des Postes et Télécommunications	P&T LUXEMBOURG	http://www.pt.lu/
Telindus S.A.	telindus	http://www.telindus.lu/

Certificate Requirements

To use the LuxTrust card, the user has to install the Middleware LuxTrust. The middleware is available under https://www.luxtrust.lu/index.php?id=196.

Application programming interface for online-verification

n.a.

2.17.4 Summary

Table 63 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 63: Summary and rating, Luxembourg, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2000.	A
technical standard	eGov, no eGov application uses eS, only VAT system uses simple signature eGov, using only weak authentication via username/passoword, PKI eInvoices: only 113% of enterprises receive orders electronically only one CSP, no intended to issue qualified certificats no central eID infrastructure eID cards will be issued in the beginning of 2008 several card readers recomended	C
distribution	no eGov application uses eS In Luxembourg, only 13 % of enterprises receive their orders electronically. No statistics on the current use of electronic signatures	-

2.18 Malta

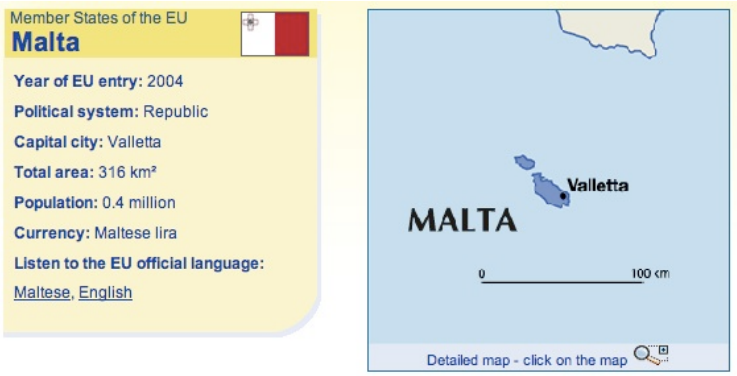


Figure 61: Fact-sheet: Malta, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:52

In figure 61 some basic demographic and geographic data of the country is presented.

2.18.1 Institutional frame

Legislation

On the 10th of May 2002, the Maltese Electronic Commerce Act (see Appendix – Malta: eCommerce Act) came into force.[563]

A subsidiary Legislation is the E-Commerce Regulations (see Appendix – Malta: Electronic Commerce Regulations).

Availability of Online-Services

•eGovernment:

Malta wants to obtain a first-class information society so the government tries to establish an e-Government in Malta and started an e-Government initiative. The Government established relationship with the local ICT sector for developing and implementing electronic services. The Government's IT Agency MITTS Ltd. is going to provide a platform for launching all electronic services. Supported by CIMU, the Central Information Management Unit, Malta wants to achieve an e-Government application that is world-class seamless.

Over 15 electronic transaction-based services are provided, like the application for certificates of birth, marriage or death. Also income tax returns can be submitted or paid and many more services are developed continuously.[564]

[563] cf. Correspondence with Stephanie Scicluna, Consumer Affairs Officer, Malta Communications Authority

[564] cf. http://www.gov.mt/egovernment.asp?p=105&l=1, access on 26.06.2007, 22:02

Another significant milestone was the implementation of the governmental Portal (http://www.gov.mt).[565] The main page can be seen in figure 62.

To identity of citizens that are transaction with Government on-line can be registered and authenticated by a mechanism that provides a secure digital signature.[566]

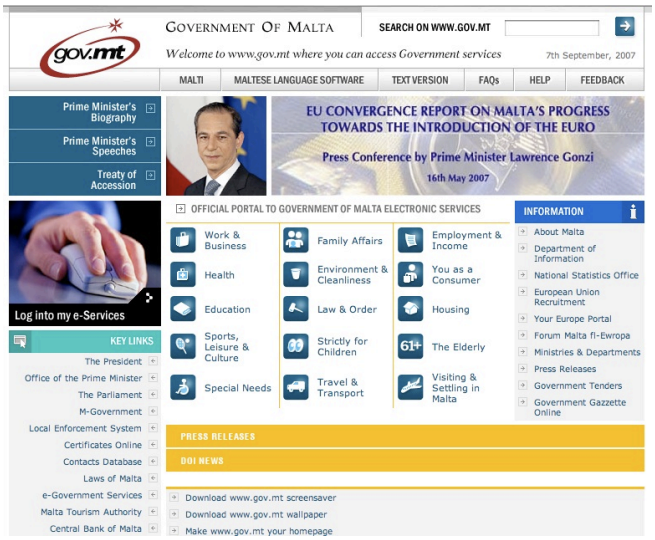


Figure 62: eGovernment portal, Malta, source: http://www.gov.mt, access on 05.09.2007, 18:35

Some of the eGovernment services use eID-authentication (table 64).

Table 64: eGovernment Services Using an eID-based authentication, source: European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Malta, April 2007, source: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Minitry for the Family and Social Solidarity	
eServices	www.mfss.gov.mt
Minitry for Health, the Elderly and Community Care	
eHealth Portal	www.eHealth.gov.mt
Ministry for Justice and Home Affairs	
Online Renewal of Passports	http://www.passaporti.gov.mt
Ministry of Finance	
Corporate taxes Online Services	http://www.ird.gov.mt
Order of Fiscal Receipts Books	http://www.vat.gov.mt
Final Settlement System	http://www.ird.gov.mt
VAT Online Services	http://www.vat.gov.mt

[565] cf. http://www.gov.mt/egovernment.asp?p=105&l=1, access on 26.06.2007, 22:02

[566] cf. http://www.gov.mt/egovernment.asp?p=105&l=1, access on 26.06.2007, 22:02

Types of electronic signature

In Malta, basic and secure electronic signatures are used. Banks prescribe a secure key and eGovernment is enabled by the use of smart chips.[567]

But the usage is not very diffused in Malta as the most services only use simple username/password method.[568]

2.18.2 Application requirements

Types of certificates

Currently, basic and non-qualified certificates are distributed publicly. Banks engage a secure key instrument with pin verification and government has own chip enabled security systems for a secure use of e-Government services.[569]

Qualified digital certificates will be distributed to all citizens on the Electronic Identity Card, which will be rolled out during 2007. The authentication mechanism of the ID card is based on digital certificates.[570]

Certification Service Providers

Currently there is no Certification Service Provider in Malta that delivers qualified certificates[571] to the general public.

The Government plant to provide all Citizens with an electronic Identity Card during 2007. This new card should contain qualified digital certificates and replaces the actual Identity Cards.[572]

The Certification service that is supported by the E-ID card is provided by the Malta Information Technology and Training Services Ltd (MITTS Ltd.).

Table 65 lists up all certification service providers in Malta:

---

[567] cf. Correspondence with Stephanie Scicluna, Consumer Affairs Officer, Malta Communications Authority

[568] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Malta, April 2007, source: http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[569] cf. Correspondence with Stephanie Scicluna, Consumer Affairs Officer, Malta Communications Authority

[570] cf. http://ec.europa.eu/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm#malta, access on 26.06.2007, 23:12

[571] cf. http://ec.europa.eu/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm#malta, access on 26.06.2007, 23:12

[572] cf. http://ec.europa.eu/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm#malta, access on 26.06.2007, 23:12

Table 65: Certification Service Provider in Malta, source: own illustration

Certification Service Provider		Issued Certificates
Malta Information Technology and Training Services Ltd.	MITTS	qualified digital certificates for eID card

Inspecting authorities

The sector of e-Commerce and electronic communication is regulated by the Malta Communications Authority (MCA).

➡Short description: Malta Communications Authority

The MCA was established on in January 2001 to regulate e-commerce and electronic communication. Its target is to achieve market competition and monitors and guides the markets it regulates. The Communications Authority is responsible for Certification Service Providers. Hence, any business whishing to proceed with becoming a CSP has to abide by certain regulations that are specified in the eCommerce Regulations (General) 2006.[573]

The National Accreditation Body is the Malta Standards Authority.

2.18.3 Technical preconditions

Signature Software

Signature Software is not applicable.[574]

Types of secure signature-creation device

Smartcards serve as Secure Signature Creation Device.

Prepayment Solutions, an Australian company that has specialized on electronic payment and secure credit card processing chooses Malta as a launch pad for a new product - smartcarde.com. The new developed smartcard technology ensures the Internet user protection of personal details, nothing is given out via the Internet. It offers a secure method for making transactions on the Internet. By purchasing a smart card, the transaction takes place in a secure environment. The user enters a Pin number and a valid authentication will be effected as the card's Public Key is matched to the PIN number. For trading transactions, a direct debit authorization and a digital signature are generated. A digital Signature is attached to each transaction.[575]

[573] cf. Correspondence with Stephanie Scicluna, Consumer Affairs Officer, Malta Communications Authority

[574] cf. Correspondence with Stephanie Scicluna, Consumer Affairs Officer, Malta Communications Authority

[575] cf. http://business-line.com/business-weekly/archieves/362/04.htm, access on 27.06.2007, 12:23

•eID card:
During 2007 all Citizens are equipped with an Electronic Identity Card that replaces the mandatory IID card and contains qualified certificates. The Card is issued by Malta‘s government.

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

2.18.4 Summary

Table 66 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 66: Summary and rating, Malta, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2002.	A
technical standard	eGovernment initiative, over 15 electronic transaction based services are provided, no eGov application uses digital signatures basic and secure eS, currently no qualified certificates, smartcards eID cards shall be distributed to all citizens, no CSP that issue qualified certificates	C
distribution	eID card for all citizens, rollout 2007, no CSP for qualified certificates, basic and secure eS is used on smart cards, but use is not very diffused in Malta as most services only use simple username/password method use of digital signature not wide spread, no eGov application uses digital signature	C

2.19 The Netherlands

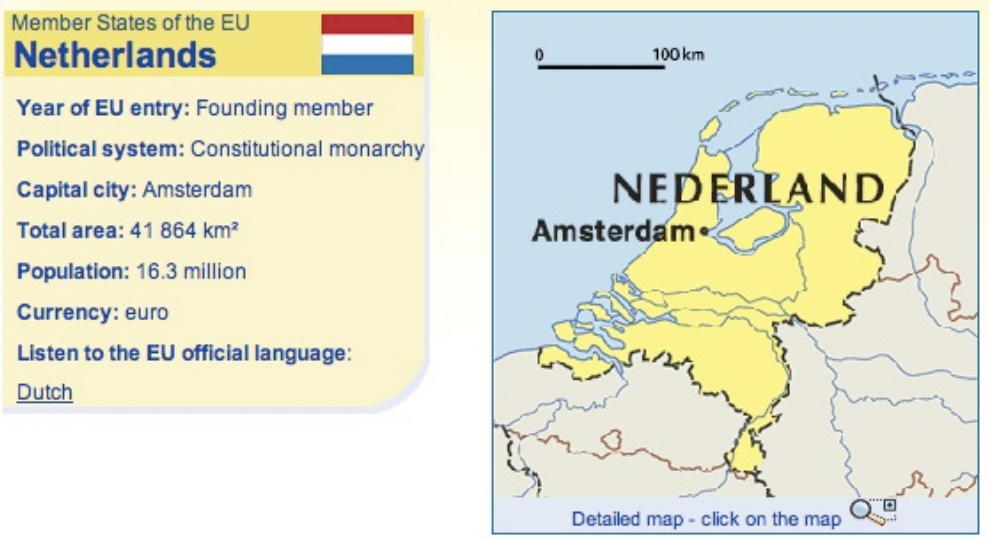


Figure 63: Fact-sheet: Netherlands, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:52

In figure 63 some basic demographic and geographic data of the country is presented.

2.19.1 Institutional frame

Legislation

On the basis of the EU-directive on Electronic Signatures, the Dutch civil code, the Las on telecommunication and the Law „Wet op economische delicten" were modified on the 8th of May 2003 (see Appendix – The Netherlands: Law on electronic signatures).[576]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Netherlands: National Regulations Details.[577]

•recognition of foreign certificates:[578]:

In March 1998, the agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:

Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden,

[576] cf. http:/www.digid.nl/english, access on 04.08.07, 16:11

[577] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[578] cf. Study of the Donau Universität Krems, Master-Studie, Austria

Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

The primary agreement for reciprocal recognition of It security certificates on basis of Common Criteria up to the evaluation grade EAL4 in October 1998 was not signed. The country has not joined the Common Criteria Mutual Recognition Agreement yet.

Availability of Online Services

•eGovernment

The Netherlands was one of the first European countries to initiate eGovernment.[579]
The eGovernment plays an important role in the Netherlands. Already in 1994 a National Action program for Electronic Highway was developed, followed by the National Action program for Electronic Government 1998 and the Digital Delta - Netherlands Online.[580]

In 2006, the government decided to invest 55 million Euro into eGovernment.[581]

A system was developed to supply a connection to local authorities and enable secure electronic transactions via the Internet. The website of this system is to find at http://www.digid.nl.

➡Short description: DigiD
DigiD was implemented by GBO.Overheid (Gemeenschappelijke Beheerorganisatie) in cooperation with the Dutch Tax Authorities.

The system of DigiD (that stands for Digital Identity) is shared between different governmental agencies to allow authentication of identity of a person that makes transactions via the Internet. The user of the services, offered by the governmental agencies, first logs onto the system with his own login code (name and password) a secure connection using Secure Socket Layer (SSL) is safeguarded and then the can get in contact with a range of governmental bodies. The design of the portal can be seen in figure 64.

The number of public authorities that implement this DigiD system is increasing. A list of participation authorities can be seen at http://www.digid.nl/burger/over-digid/wie-doen-mee.[582]

---

[579] cf. http://www.e-overheid.nl/e-overheid/geschiedenis/#Nederlandenegovernment, access on 03.12.2007, 14:18

[580] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Netherlands, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[581] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Netherlands, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[582] cf. Correspondence with Dkfm. Wolfgang Malek and Dr. Günther Mühlberger, commercial attaché for the Netherlands, Federal Economic Chamber, foreign trade office Den Haag

Also the number of inquiries via DigiD rises constantly. Over DigiD, it is possible to electronically request for children's‘ allowance or retirement pension at the social insurance system. Also the tax declaration can be handed in electronically at the Tax Authorities.[583]

Figure 64: DigiD Netherlands, source: http://www.digid.nl/, access on 05.09.2007, 18:47

In the Netherlands, also a PKI was developed, PKIoverheid. It was designed to enable secure electronic communication within the government. GBO.Overheid supports the management and control of this system.

➡Short description: GBO.Overheid[584]
GBO.Overheid is the governments‘ shared service organization that has been established to administrate some e-government services, for example the administration of DigiD, the authentication service or building an infrastructure for exchanging data via the government transaction portal. GBO.Overheid is responsible for the overall management (tactical, operational, cost-effective) of the generic key-services for e-Government, providing a constant quality.

•eTax:
Sending tax declarations via Internet has become more and more common in recent years. Since January 2005, businesses must file their tax declaration electronically. Citizen can also send their declaration electronically, from 2007 thei must use DigiD.
The electronic forms for the declarations can be downloaded from

- http://www.belastingdienst.nl/zakelijk/aangifte.html for citizens
- http://www.belastingdienst.nl/particulier/aangifte.html for businesses.

[583] cf. Correspondence with Dkfm. Wolfgang Malek and Dr. Günther Mühlberger, commercial attaché for the Netherlands, Federal Economic Chamber, foreign trade office Den Haag

[584] cf. http://gbo.overheid.nl/english, access on 04.08.07, 16:14

Citizens are not obliged to make electronic declarations, but if they decide to, DigiD must be used. Businesses can also use DigiD and use internet forms. If they use their own administration software, they can ask for name and password or use digital signatures.[585]

Over a million electronic signatures are used for this applications each year.[586]

•other eServices:
All operational and planned eGovernment applications are summed up in the Appendix - Netherlands: Operational and planned applications. [587]

Types of electronic signature

A range of municipalities, the employment centre and the land registry office are already working with use of digital Signature. On the website http://www.egem.nl, a list of organizations using digital signature can be found. EGEM was founded in cooperation between the Dutch Ministry of Interior and the Coalition of the Dutch municipalities to improve the electronic services.[588]

2.19.2 Application requirements

Types of certificates

•eID:
In August 2004, a pilot test of a new ID card was launched, the electronic Dutch Identity card (eNIK). This new card features an RFID chip that stores biometric data and digital certificates that enable holders to securely access the transactional e-government services. By 2007, the new e-ID card should have replaced the current ID card.[589] But before the card can be introduced, a control and application system must be set up first.[590]

SDU Identification supplies the new e-ID cards and generates digital certificates along with key pairs and loads these onto the chip of the smart card. This constitutes a pocket-sized digital secured system that

---

[585] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Netherlands, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[586] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Netherlands, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[587] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[588] cf. Correspondence with Dkfm. Wolfgang Malek and Dr. Günther Mühlberger, commercial attaché for the Netherlands, Federal Economic Chamber, foreign trade office Den Haag

[589] cf. http://www.libertysecurity.org/article520.html, access on 04.08.07, 16:55

[590] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Netherlands, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

enables secure usage of e-Government applications.[591]
Altogether three certificates are used for the electronic signature, confidentiality and for identity. The card is EAL4+ certified, the highest level of Common Criteria (ISO15408).
To use eNIK, a card reader is required and the facilities must support advanced electronic signature. With eNIK, all eGovernment services can be used.[592]

•Trusted Identity Manager:
DigiNotar offers a solution called Trusted Identity Manager to reduce the risk of digital communication. An Organization is provided with certificates to ensure that only certain users have access to documents or the whole system. With the Trusted Identity Manager, the organization can provide its relations with high-quality certificates. To enable the issuing of these certificates, DigiNotar provides the organization with its own Certification Authority, which issues its own Organization certificates. The certificates can be included on soft token, smart cards of USB token and can be designed consistent with the branding of the organization (own logo, color layout).[593]

Certification Service Providers
The new e-ID card is supplied by SDU Identification.

➡Short description: SDU Identification[594]
SDU Identification was established in 1994 as a competence centre of developing and manufacturing of identity documents. It specializes in the production and management of identity and financial documents. The range of products developed by SDU Identification includes passports and identity documents, memory chip cards or smart cards. It also generates and manages the use of digital certificates, using a PKI that is based on smart card technology.

➡Short description: DigiNotar[595]
DigiNotar is an independent Internet Trust Service company that supplies trust and security solutions. like electronic signatures, secure document exchange, electronic archiving and identity management. It also offers different types of identification resources, like systems with username and password use, identification solutions via mobile phone or bank card, or electronic signatures on smart cards.[596]
DigiNotar serves as an accredited certification service provider that offers qualified certificates.

In 2002, PinkRoccade and KPMG introduces electronic signature in the Netherlands. The Dutch Accreditation Council accredited KPMG Certification to certificate ICT-service provider for issuing qualified

---

[591] cf. http://www.sdu-identification.nl/eng/frmover.html, access on 04.08.07, 20:36

[592] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Netherlands, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[593] cf. http://www.diginotar.com/Default.aspx?tabid=95, access on 04.08.07, 20:39

[594] cf. http://www.sdu-identification.nl/eng/frmover.html, access on 04.08.07, 20:36

[595] cf. http://www.diginotar.com, access on 04.08.07, 19:50

[596] cf. http://www.diginotar.com/Default.aspx?tabid=89, access on 04.08.07, 21:09

certificates for electronic signature. PinkRoccade is the first and only party that issues advanced electronic signature.[597] PinkRoccade serves as accredited Certification service provider that offers qualified certificates.[598]

There is another accredited certification service provider that issues qualified certificates: CIBG.

Since 23.August 2006, also ESG De electronische signatuur BV offers its services.

Table 67 lists up all certification service providers in the Netherlands.

Table 67: Certification Service Provider in the Netherlands, source: own illustration

Certification Service Provider		Issued Certificates
SDU Identification	Sdu IDENTIFICATION	n.a.
DigiNotar	DigiNotar Internet Trust Services	qualified certificates
PinkRoccade	Getronics PinkRoccade	qualified certificates advanced certificates
CIBG	CIBG	qualified certificates
ESG De electronische signatuur BV	ESG	personal certificates

Inspecting authorities

The Body responsible for voluntary accreditation is ECP.

The Body for supervision of electronic signature issues is the Post and Telecommunications Authority.

2.19.3 Technical preconditions

Signature Software

AET offers a software package called SafeSign to increase the security. The software can initialize and use tokens for encryption, authentication and digital signature. It can define Pins, generate keys and integrate certificates.[599]

SafeSign supports the following operating systems: Windows 2000, Windows XP, Windows Vista, Windows 2003 Server, Windows XP Embedded, Windows CE (.NET) 4.2, Windows CE (.NET) 5.0, Windows Mobile 2005, Windows Mobile 5.0, Windows Pocket PC 2003, Linux, Mac OS X, Sun Solaris.[600]

---

[597] cf. http://www.egov.vic.gov.au/index.php?env=-innews/detail:m1184-1-1-8-s-0:n-146-1-0--, access on 04.08.07, 21:12

[598] cf. http://www.pinkroccade.nl, access on 04.08.07, 21:23

[599] cf. http://www.diginotar.nl/Portals/7/Handleidingen/Installation%20Guide%20SafeSign%20v4.0.pdf, access on 25.08.07, 23:15

[600] cf. http://www.aeteurope.nl/SafeSign/SafeSign_Identity_Client_Specifications, access on 25.08.07, access on 23:24

DigiNotar offers a web service infrastructure, the DigiNotar Signing Service, which enables to digitally sign official documents and forms that are transacted via the Internet. The DigiNotar environment puts a signature on documents and checks the validity of authentication. The documents are provided in PDF or XML format.
Signed documents can also be received and validated by a proof of receipt that includes a time stamp.
The DigiNotar Service can be integrated in every website.[601]

Types of secure signature-creation device

SDU Identification offers Smart cards (PKI cards) that serve as an electronic identity document (figure 65). This card includes an RFID chip that can store biometric data of the holder as well as digital certificates and key pairs for a secure use of e-Government and e-Commerce applications.[602]

Figure 65: PKI-Card, Netherlands, source: http://www.sdu-identification.nl/eng/frmover.html, access on 04.08.07, 20:36

DigiNotar offers a certification solution (Trusted Identity Manager) that enables an organization to provide its relations with own certificates. These relation certificates can be stored on soft token, smart cards of USB token.[603]

For the software SafeSign that is offered by AET the following tokens are supported (table 68):

Table 68: supported tokens for SafeSign software, AET, source: http://www.aeteurope.nl/SafeSign/SafeSign_Identity_Client_Specifications, access on 25.08.2007, 23:24

Type	model
USB Tokens	Marx CrypToken MX2048
	Starkey 100
	Starkey 200
	Starkey 220 HID
	Starkey 400
	Starsign Biotoken 3.0
Smart Cards	Starcos SPK 2.3
	Starcos SPK 2.4
	STARCOS 3.0

[601] cf. http://www.diginotar.com/Default.aspx?tabid=93, access on 04.08.07, 20:38

[602] cf. http://www.sdu-identification.nl/eng/frmover.html, access on 04.08.07, 20:36

[603] cf. http://www.diginotar.com/Default.aspx?tabid=95, access on 04.08.07, 20:39

Type	model
	Multos
	TCOS
Java Card v2.11/OpenPlatform 2.01 compliant Java cards:	Axalto Cyberflex
	G&D Sm@rtcafe Expert v2.0
	G&D STARSIM Java
	Gemplus GemXpresso Pro R3
	IBM JCOP 20/21/30/31
Java Card v2.2+ / Global Platform 2.1.1 compliant Java Card	G&D Sm@rtcafe Expert 64K
	G&D Sm@rtcafe Expert 3.0
	IBM JCOP 21/31/41 (72K)
	Oberthur IDone Cosmo64 v5.2
Multos cards	KeyCorp Multos v4.2 48K Card
	KeyCorp Multos v4.2 64K Card

Card readers

For the SafeSign software, any smart card reader is supported (table 69):[604]

Table 69: supported tokens for SafeSign software, AET, source: http://www.aeteurope.nl/SafeSign/SafeSign_Identity_Client_Specifications, access on 25.08.2007, 23:24

Type	model
smart card readers	GemPlus
	Omnikey (Cardman range)
	SCM Microsystems
	Towitoko
Secure Class 2/3 pin pad readers	G&D CashMouse/SCM STR 391
	Omnikey CardMan Trust (3621/3821)
	Reiner SCT Cyberjack pin pad
Smart card keyboard	Cherry Smartboards (G83-6744, G83-14400)
Contactless readers	Integrated engineering (SmartLOGON)
	Omnikey Cardman 5121

Certificate requirements

n.a.

Application programming interface for online-verification

DigiNotar and CIBG offer an CRL as well as an OCSP service on their website.

[604] cf. http://www.diginotar.nl/Portals/7/Handleidingen/Installation%20Guide%20SafeSign%20v4.0.pdf, access on 25.08.07, 23:15

2.19.4 Summary

Table 70 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 70: Summary and rating, The Netherlands, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2003.	A
technical standard	eGovernment (DigiD), secure transaction via Internet, advanced signature qualified certificates eID card, Smart cards, several card readers recommended, , CRL and OCSP service	A
distribution	Number of electronic inquiries via DigiD is rising, eTax: over a million eS are used each year many organizations already use digital signature	A

2.20 Poland

Figure 66: Fact-sheet: Poland, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:53

In figure 66 some basic demographic and geographic data of the country is presented.

2.20.1 Institutional frame

Legislation

In Poland, the Law on electronic signatures entered into force on 17.09.2001. It was underwritten by the state president via digital signature[605] (see Appendix - Poland - Act on electronic signature)[606].

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Poland: National Regulations Details.[607]

Availability of Online services

•eGovernment:[608]

In Poland there is no single access point for citizens and they must use many portals to gather information. There is no independent initiative for an universal mature roll-out of eGovernment systems. A

[605] cf. Correspondence with Dr. Rudolf Thaler, commercial attaché for Poland, Federal Economic Chamber, foreign trade office Warsaw

[606] cf. http://www.mgip.gov.pl/NR/rdonlyres/9C534966-8336-49C9-8087-0F4A64F14D66/18224/act_on_eSignature.pdf, access on 03.12.2007, 14:26

[607] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[608] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Poland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

project was launched „Wrota Polski“, the Gateway of Poland.[609] Also the ePUAP portals are developed that are also part of the Gateway (figure 67):

Figure 67: ePuap portals, source: http://www.e-puap.mswia.gov.pl/, access on 03.12.2007, 14:27

ePUAP has been originated with the aim to create interactive electronic services that are based on user identifications and authentication as well as on electronic signatures.[610]

But the Gateway of Poland as well as ePUAP have not yet implemented completely. Local public administration authorities create their own informative portals.[611]

•eTax:[612]

The Ministry of Finances planned to develop an electronic tax system, enabling taxpayers to transmit their tax returns electronically. The System is called e-podatki[613] and is one of the scopes of the Ministry‘s activities.

The project e-Deklaracje was part of the e-podatki project and aimed to create a system for direct communication between external authorities and tax administration. in August 2006, the system e-poltax was made accessible for about 7.500 entities. The complete roll out is planned during 2008.

To use the e-poltax system, electronic documents must be provided with a secure electronic signature verified by a valid qualified certificate.

---

[609] for more information see http://www.mswia.gov.pl/index.php?dzial=267&id=3897

[610] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Poland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[611] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Poland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[612] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Poland, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[613] see https://e-poltax.mf.gov.pl

•other eServices:
All operational and planned eGovernment applications are summed up in the Appendix - Poland: Operational and planned applications.[614]

Types of electronic signature

Electronic signature does exist in Poland, but only few people have bought one. One reason is that the possibilities of application of electronic signature are limited. Also the Polish departments are not prepared for that innovation. The Government was to implement electronic signature in all public departments last year, but must delay the appointment to May 2008.

According to Gazeta Prawna (http://www.gazetaprawna.pl) the number of assigned signatures is estimated for 10.000 to 15.000. These signatures have been issued only to natural persons.[615]

The value of the market is estimated to about some hundred thousand up to one Million PLN per year. But the market will develop next year, as all companies with more than five employees must use an electronic signature when transferring documents to the social insurance institution.

Currently two types of electronic signatures are in use: basic and secure signature.

The development of the market is being blocked by tree factors:

- lack of knowledge
- high costs of electronic signatures (from 300 to 500 PLN) and
- little number of services, that works with electronic signatures.

Summed up, there are fewer incentives to implement electronic signatures for citizens.[616]

In December 2005, The BOS S.A., the Bank Ochrony Srodowiska SA, offers its clients to use safe electronic signature under the electronic banking system. The Bank is in the leading market position as it is the first bank that has introduced such a system.[617]

The Certification Service Providers, Unizeto and Sigillum, issue qualified certificates for a secure electronic signature.

---

[614] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[615] cf. Correspondence with Dr. Rudolf Thaler, commercial attaché for Poland, Federal Economic Chamber, foreign trade office Warsaw

[616] cf. Correspondence with Dr. Rudolf Thaler, commercial attaché for Poland, Federal Economic Chamber, foreign trade office Warsaw

[617] cf. http://www.bosbank.pl/i.php?i=545, access on 27.06.07, 10:18

2.20.2 Application requirements

Types of certificates

Unizeto, one of the Certification Service Providers, issues qualified certificates for a secure electronic signature, also non-qualified certificates for e-signature, data encryption etc.[618]

Sigillum PCCE, the Polish Centre of Electronic Certification, offers basic sets for qualified digital signature, that contain two certificates:

- Sigillum Top qualified certificate,
- Sigillum Basic commercial certificate.[619]

Certification Service Providers

The Ministry for Economic Affairs awarded the Polish National Bank the function of the main office for electronic signature. The Narodowe Centum Certyfikacji, the national certification centre (http://www.nccert.pl), is resident at the national bank and administrates the register of all certifications service providers. The centre also publishes the List of the assigned certificates and of those certificates that had become void.[620]

Currently, there are three Certification Service Providers in Poland: Krajowa Izba Rozliczeniowa, Unizeto and Wytwornia Papierow Wartosciowych (Polish Security Printing Works).

Unizeto issues qualified certificates for a secure electronic signature, offers authenticity verification of documents that are electronically signed. Also a certificate status verification is supported by Unizeto. [621]

The services concerning digital signature are provided by the Wytwornia Papierow Wartosciowych through Sigillum PCCE, the polish centre of electronic certification.[622]

Sigillum offers basic sets for qualified digital signature, it provides signatures to public (eAdministration) as well as business companies (e.g., eBanking, eInvoice).[623]

Table 71 lists up all certification service providers in Poland.

---

[618] cf. http://www.unizeto.pl/unizeto/uni,aboutus_about_company.xml, access on 08.08.07, 12:01

[619] cf. http://www.sigillum.pl/sig-cmsws/page/?F;214, access on 08.08.07, 12:03

[620] cf. Correspondence with Dr. Rudolf Thaler, commercial attaché for Poland, Federal Economic Chamber, foreign trade office Warsaw

[621] cf. http://www.unizeto.pl/unizeto/uni,aboutus_about_company.xml, access on 08.08.07, 12:01

[622] cf. http://www.sigillum.pl, access on 08.08.07, 12:03

[623] cf. Correspondence with Krzysztof Wisniewski, PWPW Poland

Table 71: Certification Service Provider in Poland, source: own illustration

Certification Service Provider		Issued Certificates
Krajowa Izba Rozliczeniowa		n.a.
Unizeto Certum		qualified certificates
Wytwornia Papierow Wartosciowych		qualified certificates basic commercial certificates

Inspecting authorities

The Body responsible for supervision and accreditation is the Ministry of Economy.

2.20.3 Technical preconditions

Signature Software

n.a

Types of secure signature-creation device

In 2006, Bull implemented a CitiCard for the Polish city Rybnik

The CitiCard enables citizens of Rybnik to make different transactions in the information network or a public service point in the city. It is also a sort of electronic burs, enables electronic signature, and replaces the tickets for public transports or sport centers. The electronic signature is used when sending documents electronically to the municipality[624].

At the moment, a project is in development for being able to use mobile phones for accessing public and private online-services. The User should be identified by the SIM-Cards. So far, the Services have failed because of complications of the user-identification. The distribution of electronic signatures was also not possible because many online services of the government do not accept digital signature.[625]

The Certification Service Provider Unizeto recommends different smart cards (table 72):

Table 72: offered smart cards, source: http://www.unizeto.pl/unizeto/uni,offer_cards.xml, access on 08.08.2007, 13:13

Provider	Smart card		Technical Parameters
Unizeto	Unizeto cryptoCertum		chip: Philips, memory: 32 Kbytes, cryptography: symmetric (DES, 3DES), asymmetric (DSA, RSA), protocols: T=0 and T=1.

[624] cf. http://www.bull.com/bulldirect/N8/rybnik.html, access on 27.06.2007, 10:25

[625] cf. http://www.poland.gov.pl, access on 27.06.07, 11:34

Pro-vider	Smart card		Technical Parameters
	Giesecke & Devrient Starcos S2.5		chip: Philips, memory: 8 Kbytes, also available: 4, 16, 32 Kbytes, cryptography: symmetric (DES, 3DES).
	Giesecke & Devrient Starcos SPK2.3		chip: Philips, memory: 32 Kbytes, cryptography: symmetric (DES, 3DES), asymmetric (DSA, RSA), protocols: T=0 and T=1
	Giesecke & Devrient Starcos SPK2.4		chip: Philips, memory: 32 Kbytes, cryptography: symmetric (DES, 3DES), asymmetric (DSA, RSA), protocols: T=0 i T=1.
	Giesecke & Devrient Starcos SPK2.5DI		Within the contact part: depending on the chosen system in the contact part (see STARCOS® SPK2.3/2.4). Within the non-contact part: chip: Philips Mifare ProX / Infineon, memory: 16 Kbytes / 32 Kbytes, cryptography: symmetric (DES, 3DES), asymmetric (RSA), protocols: T=0, T=1, T=CL.
	Giesecke & Devrient Starcos SPK3.0		Technical parameters chip: Philips Smart MX memory: 72 Kbytes, 36 Kbytes available at client's request, cryptography: symmetric (DES, 3DES), asymmetric (RSA-CRT with keys - the length of 2048 bits), protocols: ISO 7816-3 T=0 i T=1.
	Giesecke & Devrient Sm@rtCafe Expert		chip: 16-bit high security microcontroller, Common Criteria EAL 4+ certificate memory: 64 Kbytes EEPROM protection: symmetric cryptography (DES, 3DES, AES), asymmetric cryptography (RSA up to 2048 bits, DSA up to 1024 bits, RSA generated on a card – up to 2048 bits), DSA keys generated on a card, crushing function algorithms: MD5, SHA–1, RIPEMD-160, electronic signature with symmetric encryption (DES Mac, ISO 9797M1, ISO 9797M2, PKCS#5 AES Mac), electronic signature with asymmetric encryption (RSA z SHA–1, PKCS#1, RFC2409, RSA with MD5, PKCS#1, RFC2409, RSA with RIPEMD–160, ISO 9796, PKCS#1, DSA with SHA–1, FIPS 186–2 DSS), DAP verification (multiple, upon request, with the use of RSA or 3DES), cryptographic algorithms effective in the protection against: SPA, DPA, DFA, firewall for the application protects against: DFA, program attacks. security domains, encrypted confidential data interception (e.g., PIN, keys, etc.).

Pro-vider	Smart card		Technical Parameters
			supported software: StarSign® Token for Java™, ActivCard Gold™, AET SafeSign. available applets: identification, PKI, one-time passwords, loyalty programs, additional applications upon request.

Card readers

The Certification Service Provider Unizeto offers a range of card readers, connected trough RS232, USB or PCMCIA and recommends the following card readers (table 73):

Table 73: recommended smart card readers, source: http://www.unizeto.pl/unizeto/uni,offer_readers.xml, access on 07.08.2007, 08:02

Mark (Models)		connection	supported operating system	supported cards
Omnikey Card-Man 1010		RS232 port	Win 95: YES, Win 98: YES, Win NT4: YES, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: NO, Win CE 3.0/NET: NO, Linux: upon request, Unix: upon request, Mac OS X: NO	all cards using protocols T=0 and T=1, microprocessor cards, no memory card support.
Omnikey Card-Man 2011		RS232 port	Win 95: YES, Win 98: YES, Win NT4: YES, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: NO, Win CE 3.0/NET: NO, Linux: upon request, Unix: upon request, Mac OS X: NO.	all cards using protocols T=0 and T=1, SLE4418/28, SLE4432/43, all I2C cards.

Mark (Models)		connection	supported operating system	supported cards
Omnikey Card-Man 3021		USB	Windows 98/ME, Windows 2000, Windows XP, Windows 2003 Server, Windows XP64bit Linux.	all cards using protocols T=0 and T=1, microprocessor cards, no memory card support.
Omnikey Card-Man 3111		RS232 port	Win 95: YES, Win 98: YES, Win NT4: YES, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: YES, Win CE 3.0/NET: upon request, Linux: YES, Unix: upon request, Mac OS X: NO	all cards using protocols T=0 and T=1, SLE4418/28, SLE4432/43, SLE4404, SLE4442 (S=10), all I2C cards.
Omnikey Card-Man 3121		USB	Win 95: NO, Win 98: YES, Win NT4: upon request, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: YES, Win CE 3.0/NET: depending on the device, Linux: YES, Unix: upon request, Mac OS X: NO	all cards using protocols T=0 and T=1, SLE4418/28, SLE4432/43, SLE4404, all I2C cards.
Omnikey Card-Man 3621		USB	Win 95: NO, Win 98: YES, Win NT4: NO, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: YES, WinXP 64Bit Itanium: YES, WinXP 64 Bit AMD, EM64T: YES, Win CE 3.0/NET: upon request, Linux: upon request, Unix: upon request, Mac OS X: upon request	all cards using protocols T=0 and T=1, SLE4418/28, SLE4432/43, SLE4404, all I2C cards

Mark (Models)		connection	supported operating system	supported cards
Omnikey Card-Man 3821		USB	Win 95: NO, Win 98: YES, Win NT4: NO, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: YES, Win CE 3.0/NET: depending on a device, Linux: upon request, Unix: upon request, Mac OS X: upon request	all cards using protocolsT=0 i T=1, SLE4418/28, SLE4432/43, SLE4404, all I2C cards.
Omnikey Card-Man 4040		PCMCIA	Win 95: NO, Win 98: YES, Win NT4: NO, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: YES, Win CE 3.0/NET: YES, Linux: upon request, Unix: upon request, Mac OS X: upon request.	all cards using protocols T=0 i T=1, SLE4418/28, SLE4432/42, SLE4404, all I2C cards.
Omnikey Card-Man 5121 RFID		USB	Win 95: NO, Win 98: YES, Win NT4: NO, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: YES, WinXP 64Bit Itanium: YES, WinXP 64 Bit AMD, EM64T: YES, Win CE 3.0/NET: upon request, Linux: upon request, Unix: upon request, Mac OS X: upon request.	all cards using protocolsT=0 i T=1, SLE4418/28, SLE4432/43, SLE4404, all I2C cards.
Omnikey Card-Man 6121		USB	Win 95: NO, Win 98: YES, Win NT4: NO, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: YES, Win CE 3.0/NET: request, Linux: upon request, Unix: upon request, Mac OS X: upon request.	all cards using protocols T=0 and T=1, SLE4418/28, SLE4432/42, SLE4404, all I2C cards.

Mark (Models)		connection	supported operating system	supported cards
Omnikey Card-Man 7120		USB	Win 95: NO, Win 98: YES, Win NT4: upon request, Win 2000: YES, Win ME: YES, Win XP: YES, Win XP SP2: YES, Win CE 3.0/NET: request, Linux: upon request, Unix: upon request, Mac OS X: upon request.	all cards using protocols T=0 i T=1, SLE4418/28, SLE4432/42, all I2C cards
Omnikey Card-Man Finread		U SB	Win 95: NO, Win 98: NO, Win NT4: NO, Win 2000: YES, Win ME: NO, Win XP: YES, Win XP SP2: YES, Win CE 3.0/NET: NO, Linux: NO, Unix: NO, Mac OS X: NO	all cards using protocols T=0 i T=1,

Certificate requirements

n.a.

Application programming interface for online-verification

The Narodowe Centum Certyfikacji, the national certification centre, publishes the List of the assigned certificates and of those certificates that had become void.[626]

According to the law, a xAdES format has to be used to verify the authentication of an electronic signature.[627]

Unizeto offers PKI services, including issuing among others an OCSP service.[628]

[626] cf. Correspondence with Dr. Rudolf Thaler, commercial attaché for Poland, Federal Economic Chamber, foreign trade office Warsaw

[627] cf. Correspondence with Dr. Rudolf Thaler, commercial attaché for Poland, Federal Economic Chamber, foreign trade office Warsaw

[628] cf. http://www.unizeto.pl/unizeto/uni,offer_pki_software.xml, access on 07.08.07, 23:02

2.20.4 Summary

Table 74 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 74: Summary and rating, Poland, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2001. The Law was signed via ES	A
technical standard	no single access point for eGov, eGov projects, Gateway not yet implemented eTax: roll out planned during 2008 market will develop next year, all companies with more than 5 employees must use eS to submit documents to social insurance eBanking other eServices: applications of electronic signature are limited basic and advanced eS non qualified certificates, Qualified certificates for secure electronic signature; 3 CSP CitiCard, project for using mobile SIM card several types of smartcards and readers CRL and OCSP	B
distribution	Electronic signature exists, but only few people have bought it as applications for use are limited, high costs of ES, approximately between 10.000 and 15.000 signatures issued to natural persons Also Polish departments are not prepared for ES implementation of ES in public departments in 2008	C

2.21 Portugal

Figure 68: Fact-sheet: Portugal, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 68 some basic demographic and geographic data of the country is presented.

2.21.1 Institutional frame

Legislation

The electronic Signature is regulated by the Decreto-Lei n.°62/2003 that complete the Decreto-Lei n. °290-D/99 (see Appendix - Portugal: Decreto-Lei n.°62/2003, only available in Poruguese).[629]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Portugal: National Regulations Details.[630]

•recognition of foreign certificates:

In Portugal, the european agreements for mutual recognition of security certificates are in force: the Agreement for reciprocal recognition of It security certificates (SOGIS-MRA). This agreement on basis of Common Criteria was enhanced u to evaluation grade EAL7.

The primary agreement for reciprocal recognition of It security certificates on basis of Common Criteria up to the evaluation grade EAL4 was not signed by Portugal; Portugal has not joined the Common Criteria Mutual Recognition Agreement yet.[631]

---

[629] cf. Correspondence with Mag. Peter Rattinger, commercial attaché for Portugal, Federal Economic Chamber, foreign trade office Lisboa

[630] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[631] cf. European Commission, eGovernment Factsheets, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

Availability of online services

•eGovernment:[632]

In 1996, The Government launched the National Initiative for the Information Society concerning four themes:

- IT in education
- electronic business
- open administration
- knowledge.

In 2000, the Operational Programme for the Information Society (POSI) was adopted. It is was supported by the EU and covered the years 2000-2006. The goal was to develop ICT skills, introduce a Digital Portugal and offer public services online.

2003, the Action Plan for the Information Society and eGovernment Action Plan was approved.

One year later, Future 2010 - Operational Programme for the Knowledge Society was presented to promote a public sector reform and further the use of ICT and eServices.

In March 2004, the new Citizen‘s Portal, the new eGovernment Portal was launched (Portal do Cidadao, figure 69).

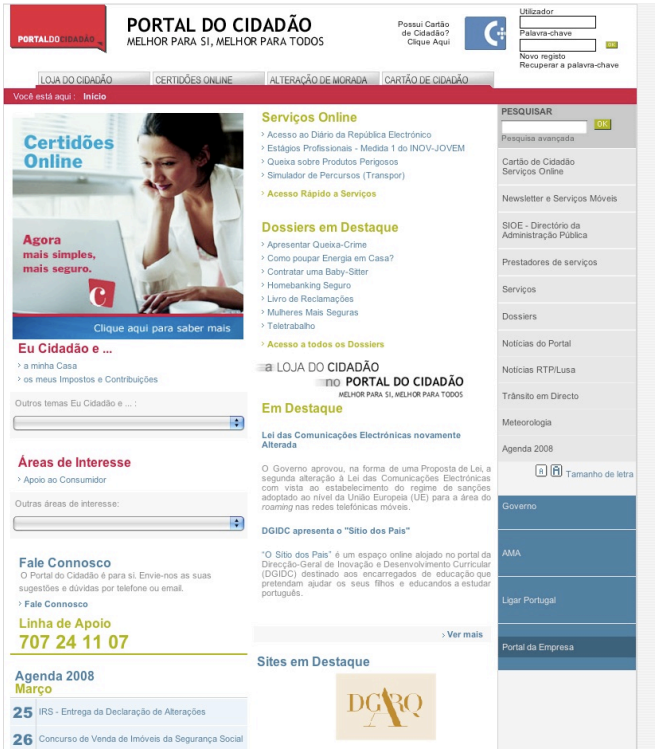


Figure 69: Citizen‘s Portal - Portal do Cidadao, source http://www.portaldocidadao.pt/PORTAL/pt, access on 04.12.2007, 17:12

[632] cf. European Commission, eGovernment Factsheets, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

The Portal replaces the the former Incocid Portal and targets citizen but also businesses, featuring different services and user registration.[633]

In August 2005 a lot of other initiatives have started:[634]

- development of mobile payment systems
- eTicketing system for public transport,
- electronic identification system for cars,
- general use of ICT in public administration,
- implementation of eHealth services,
- development of eVoting,
- Improvement of criminal investigation.

•e-Procurement:
2005, the national e-procurement portal (Portal de Compras) was launched, promoting transparency of public sector, encouraging eCommerce and increasing productivity and competitiveness of businesses in Portugal.[635]

•eInvoicing:[636]
The Portuguese Government decided to implement mechanisms to enable eInvoices within the cabinets and between the institutions. Actually, platforms for eInvoices have been implemented in 12 cabinets and are being tested with about 40 institutions. Those systems require the use of advanced electronic signatures or en eID.

•eVoting:
Portugal started a range of projects for electronic voting with the goal to enable citizen to vote electronically. The first pilot was started in 2004 during the European Elections, testing tree different technologies, including 150 000 voters, applied in 9 municipalities.
In 2005, voting platforms have been improved for Legislative Elections. Also citizens living abroad were able to test electronic intern voting (From 38 countries 4500 people participated).
The both projects were not binding but used for university evaluations, which were very positive.[637]

---

[633] cf. European Commission, eGovernment Factsheets, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

[634] cf. European Commission, eGovernment Factsheets, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

[635] cf. European Commission, eGovernment Factsheets, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

[636] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Portugal, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[637] cf. European Commission, eGovernment Factsheets, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

•LigarPortugal - online public services:
In July 2005, another portal was approved - LigarPortugal, a new action program for information and knowledge society. The program detains that all basic public services shall be available online by 2009.[638]

•eTax:
Since January 2006, all businesses must submit the annual income tax declaration electronically via eFinance, the government's website.[639]

•Empresa Online - business portal for online registration of companies:
In June 2006, „Empresa On-line" was launched (figure 70), a new business portal that permits an online registration of companies. The portal offers help on legal procedures and some administrative formalities.

Figure 70: Empresa On-line, Business Portal, source: http://www.portaldaempresa.pt, access on 07.01.2008, 15:46

The portal is maintained by the Directorate-General for Register and Notaries.
To access the portal, digital signatures are required. To use the portal, qualified signatures are required for the end user, lawyers, solicitors and notaries must use advanced electronic signature. The signatures are verified by the Directroate-General for Register and Notaries by OSCP and CRLs services and authorizes the incorporation of the companies.[640]

[638] cf. European Commission, eGovernment Factsheets, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

[639] for more information see http://www.e-financas.gov.pt

[640] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Portugal, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Types of electronic signature

In Portugal, all types of digital signature are used: basic signature, advanced and qualified electronic signature: digital or advanced electronic.[641]

2.21.2 Application requirements

Types of certificates

Only software certificates could be identified.[642]

Multicert CA issues high grade certificates:[643]

- SSL/TLS Webserver certificates
- Email certificates
- personal and professional certificates
- application certificates
- Code Signing certificates.

Mulitcert also provides Timestamping services.

Certipor issues the following certificates (figures 71-73):

Our Certificates - For you

Type of Certificate	Characteristics	Trust Level	Validity	Subscription Documents	Price	Fill application on-line
Individual Level 1 (N1)	A, B, C, D	Minimum	30 days	None	Free	
Individual Level 2 (N2)	A, B, C ,E	Medium	1 year	2, 3	PTE: 1804 Euro: -,-	
Individual Level 3 (N3)	A, B, C, F, G	Maximum	1 year	1, 2, 3	PTE: 3809 Euro: -,-	

Characteristics
A. Allows digital signatures on documents and e-mail.
B. Allows **secure e-mail** exchange
C. Allows **user authentication** on servers and/or services.
D. To subscribe you only need a valid e-mail account. **See subscription process.**
E. Requires signing a contract. **See subscription process.**
F. **Digital signature** with probational value.
G. Contract is signed in person. **See subscription process.**

Subscription documents
1. ID card, driver's license, or passport.
2. ID document copy.
3. Subscription contract signed as ID document.

Figure 71: Issued certificates by Certipor, source: http://www.certipor.com/para_si_eng.html, access on 07.01.2008

641 cf. Study of the Donau Universität Krems, Master-Studie, Portugal

642 cf. Study of the Donau Universität Krems, Master-Studie, Portugal

643 cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Portugal, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Our Certificates - For your company (Individual)

Type of Certificate	Characteristics	Trust Level	Validity	Subscription Documents	Price	Fill application on-line
Individual Level 2 (N2)	A, B, C, D	Medium	1 year	2, 3, 4 ,5	PTE: - Euro: -,-	
Individual Level 3 (N3)	A, B, C, E, F	Maximum	1 year	1, 2, 3, 4, 5	PTE: - Euro: -,-	

Characteristics
A. Allows digital signatures on documents and e-mail.
B. Allows **secure e-mail** exchange
C. Allows **user authentication** before servers and/or services.
D. Requires signing a contract. **See subscription process.**
F. **Digital signature** with probational value.
G. Contract is signed in person. **See subscription process.**

Subscription documents
1. ID card, driver's license or passport.
2. ID document copy.
3. Subscription contract signed according to ID document.
4. Company fiscal card copy.
5.Company authorization to issue a digital certificate.

Figure 72: Issued certificates by Certipor, source: http://www.certipor.com/para_empresa_eng.html, access on 07.01.2008

Our Certificates - For your company (Servers)

Type of Certificate	Characteristics	Trust Level	Validity	Subscription Documents	Price	Fill application on-line
Server Level 2 (N2)	A, B, C, D	Medium	15 days	2, 3, 4, 5	Free	
Server Level 3 (N3)	B, C, D, E	Maximum	1 year	1, 2, 4, 5, 6	PTE: - Euro: -,-	

Characteristics
A. Testing certificate. **See the subscription process.**
B. Web server authentication certificate.
C. Creation of secure SSL/HTTPS channels - 128 bits between server and browsers.
D. Possibility of controling access to users having digital certificates.
E. Contract signature in person. **See the subscription process.**

Subscription Documents
1. ID Card, driver's license or passport.
2. ID document copy.
3. Subscription contract (available at the moment of request submission).
4. Company fiscal card copy.
5. Company written request (in the company's stationary) to issue the digital certificate.
6. Domain record copy (Internic, or other)

Figure 73: Issued certificates by Certipost, source: http://www.certipor.com/para_servidor_eng.html, access on 07.01.2008, 15:49

The eID card contains a qualified certificate that follows the X509.v3 standards and is issued by INCM, Portuguese Mint. The fields of the certificate are listed up in Appendix - Portugal: Fields of the eID Citizen Signature Certificate.

Certification Service Providers

In Portugal, there are no private enterprises that are accredited.[644]

IBS and Saphety are operating in the area of electronic signature, but are not accredited.[645]

The Certification Service Providers are:

- IBS
- Saphety
- Certipor, S.A.
- Instituto das Tecnologias de Informacao na Justica
- Mulicert S.A.
- Entidade Certificadora Comum do Estado ECCE

Table 75 lists up all certification service providers in Portugal.

Table 75: Certification Service Provider in Portugal, source: own illustration

Certification Service Provider		Issued Certificates
IBS		n.a.
Saphety		n.a.
Certipor		individual certificates company certificates Server certificates
Instituto das Tecnologias de Informacao na Justica		n.a.
Mulitcert		SSL/TLS webserver certificates email certificates personal and professional certificates application certificates code signing certificates timestamps
ECCE		n.a.

[644] cf. Correspondence with Mag. Peter Rattinger, commercial attaché for Portugal, Federal Economic Chamber, foreign trade office Lisboa

[645] cf. Correspondence with Mag. Peter Rattinger, commercial attaché for Portugal, Federal Economic Chamber, foreign trade office Lisboa

Inspecting authorities

n.a.

2.21.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

•eID card:

In April 2005, the government launched the Citizen Card Project. Citizens shall be provided with id cards that combine tax, health insurance, social security and further information to enable citizen carrying just one card. The distribution was planned to start in 2006.[646]

But the electronic Citizen Card was then developed in February 2007 and planned to make it available by 2008. The Citizen Card is a smart card, providing identity authentication by photo and fingerprint and enabling electronic signature.[647] The design can be seen in figure 74.

This Citizen Card enables the use for identification, tax services, social security and health systems. It also permits the access to eGovernment services, including a Pin code for generation digital signatures.[648]

The card will replace the following existing cards: ID document, Tax Card, Social Security Card, Voting Card and Health System card. The Office of Public Services Reform coordinates the Card project and is in partnership with Knowledge Society Agency.[649]

Figure 74: National eID card, Poland, source: http://www.logisticsit.com/absolutenm/templates/article-datacapture.aspx?articleid=2808&zoneid=6, access on 28.11.2007, 13:113

[646] cf. European Commission, eGovernment Factsheets, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

[647] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Portugal, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[648] cf. European Commission, eGovernment Factsheets, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

[649] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Portugal, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

Certipor offers a certification revocation list on their homepage: www.certipor.com.
Multicert offers OCSP validation services as well as LDAP and CRL verification services.[650]

2.21.4 Summary

Table 76 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 76: Summary and rating, Portugal, source: own illustration

categories		rating
legal framework	Electronic Signarture are regulated since 2003.	A
technical standard	eGov, eInvoicing, eVoting all types of signatures, only software certificates, but eID card roll out in 2008 6 CSP, none accredited ID card project, available by 2008 CRL, OCSP	B
distribution	eInvoicing: within cabinets and institutions platforms implemented in 12 cabinets and tested with 40 institutions	-

[650] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Portugal, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

2.22 Romania

Figure 75: Fact-sheet: Romania, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:53

In figure 75 some basic demographic and geographic data of the country is presented.

2.22.1 Institutional frame

Legislation

The Law on electronic signatures was adopted in December 2001 (see Appendix – Romania: Law on Electronic Signatures).

•recognition of foreign certificates

Certificates issued by providers based outside Romania are recognized in Romania if:

a) the certification service provider based outside Romania has been accredited under the accreditation scheme whose establishment is stipulated by the law in question; or

b) a Romanian accredited certification service provider guarantees the certificates issued by the foreign CA; or

c) the certificate or CA that issued it is recognized under a bilateral or multilateral agreement between Romania and other states or international organizations.

At present Romania has no international agreements concerning mutual recognition of digital certificates No foreign CA is accredited in Romania.

Availability of Online Services

•eGovernment:

In the last few years, Romania has made a notable progress in the Information and Communications Technology.

The Romanian Government started a long-term project to further the electronic communication between public institutions. [651]

In 2003, the National Electronic System (SEN) was created to supply public services electronically. This IT system consists of two components, the e-government system and the e-administration system.

To give citizens the possibility to interact with the public administration of Romania, the website www.e-guvernare.ro was implemented in September 2003 (figure 76). It is as unique access point for services and information of the public administration.[652]

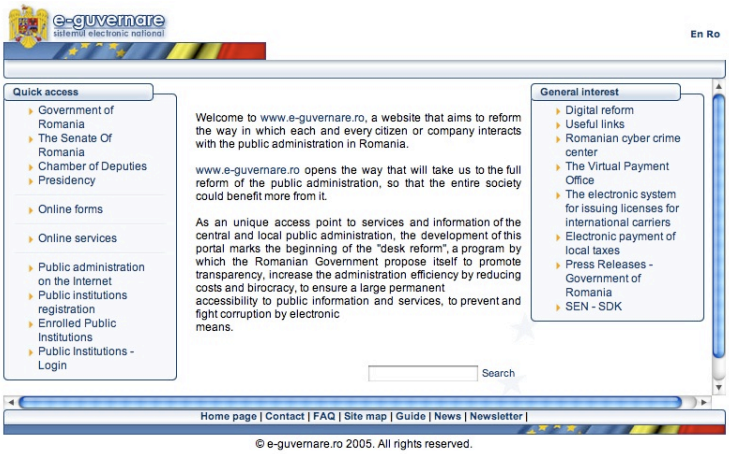


Figure 76: eGovernment, Romania, source: http:// www.e-guvernare.ro, access on 05.09.2007, 19:02

The National Electronic System SEN provides 20 public services, 12 for citizens and 8 for businesses. It was created to serve as single point sign-on. The General Inspectorate for Communications and IT (IGCTI) that operates the e-government system, is keen to implement national bridges to allow an interoperability with using digital certificates issued by IGCTI.

The responsible organization is the General Inspectorate for Communications and IT (http:// www.igcti.ro).[653]

•eTax:

Users of the National Electronic System can also send their Tax Declarations electronically that are signed electronically with a certificate. The signature is required. Since April 2005, about 45.000 tax declarations have been sent via SEN.

---

[651] cf. http://www.e-guvernare.ro/default.aspx?LangID=4, access on 09.08.07, 07:19

[652] cf. http://www.e-guvernare.ro/default.aspx?LangID=4, access on 09.08.07, 07:19

[653] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•eProcurement:[654]

In March 2002, a portal for electronic public procurement was launched under http://www.e-licitatie.ro (figure 77). The responsible organization is IGCTI, the General Inspectorate for Communications and IT (http://www.igcti.ro).

Figure 77: eProcurement Portal, source: http://www.e-licitatie.ro, access on 05.12.2007, 20:08

This application allows private companies to participate online in the public acquisition process. The Portal was only launched for some public institutions. Public institutions can publish acquisitions announcements electronically, private companies participate in the acquisitions. The whole process is fully electronic automated. To sign a contract a digital signature is required. The authentication and signing process relies on an electronic certificate that is issued by IGCTI.

Signing registration forms require a qualified electronic certificate, authentication and singing procedures use only a simple electronic certificate.

The portal recommends electronic signatures for registration process and requires signatures for the system usage.

The electronic signature is enabled by using electronic certificates issued either by IGCTI or other commercial certification authorities.

Since 2003, about 700 public institutions are interacting in the portal as contracting authorities, about 700 private companies are suppliers.

•STFD - Tranfond S.A.[655]

To easier the payment clearing and settlement services of credit institutions, the STFD system was created. Users are domestic banks, that can log on the system and transfer money electronically in a secure way. Every request and transaction is signed electronically, using qualified electronic certificates.

Every transaction demands for a signature to enforce the transaction. The system doesn‘t accept the

[654] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[655] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

transaction if the authentication procedure fails.
The responsible organization is the STFD - Transfond S-A.
The users have learned quickly how to use the application and the signature. Actually, about 10.000 signatures are used for inter banking money transfers per day.

•ROVINARI - National Energy Facility (CEN):[656]
CEN Rovinari is the main power energy supplier in Romania. Rovinari‘s employees can log into the system and sign documents and eMails electronically. Every eMail and document that is sent within the company is being signed. The authentication relies on the use of advanced signature. If the authentication fails, no operation is allowed and the system doesn‘t accept transactions. The login is enabled using a digital certificate. The certificates are installed on a secure USB token.
Per day, about 1.200 signatures are effected by CEN Rovinari employees.

•Romanian Insurance Supervisory Commission:[657]
The commission is independent and aims to provide a stable environment for the insurance market by protecting the insured‘s rights. Insurance companies can log into the system on the Insurance Supervisory Commission internal network and sign documents and eMails electronically. Every request that is sent by an insurance company is electronically signed and every eMail sent within the company is signed.
The system requires on qualified signatures for authentication, based on certificates that are issued by commercial certification authorities.
Every transaction requires the user‘s signature to enforce the transaction. The system does not allow any operation if the authentication fails.
Actually, about 800 signatures are created per day.

•other eServices:
All operational and planned eGovernment applications are summed up in the Appendix - Romania: Operational and planned applications.[658]

Types of electronic signature

The National Electronic System relies on electronic signature based on a qualified electronic certificate. The participants use their software certificates that are installed on their workstation. All tax declarations are electronically signed by the user. Companies use electronic certificates for authentication and for signing the declarations.[659]

---

[656] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[657] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[658] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[659] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

The STFD - Transfond S-A. system for the domestic banking community relies on the use of qualified signatures based on certificates that are installed on secure USB tokens.
The ROVINARI system of the National Energy Faciliy Rovinari relies on advanced electronic signatures based on certificates on secure USB tokens.
The system used by the Romanian Insurance Supervisory Commission relies on authentication by using qualified signatures based on electronic certificates on secure USB tokens.[660]

2.22.2 Application requirements

Types of certificates

Certification service providers in Romania have to provide qualified certificates.
Qualified certificates have a corresponding structure: ETSI TS 101 862 v. 1.2.1, RFC 2459 and ITU-T X. 509. The legal validity of qualified certificates is 1 year.
The structure of qualified certificates can be seen in the Appendix - Romania: Structure of Qualified Certificates.[661]

The National Electronic System relies on electronic signature based on a qualified electronic certificate. The participants use their software certificates that are installed on their workstation.
Companies use electronic certificates for authentication and for signing the declarations.[662]
The relevant certification policy can be found in the Appendix - Romania: General Inspectorate for Communications and IT Certification Policy.[663]

The Certification Service Provider TransSped has issued about 8000 certificates up to now.[664]

Certification Service Providers

In 2006, 5 certification service providers offered their services in Romania. Only two of them are accreditied.

➡short description: National Trade Register Office
The National Trade Register Office was the first to issue qualified certificates to a public institution in Romania, securing data transmissions between the central office and its territorial branches.

---

[660] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[661] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[662] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[663] cf. http://ac.e-guvernare.ro/pc/, access on 05.12.2007, 20:10

[664] cf. Correspondence with Viky Manaila, Managing Directror, Trans Sped SRL, Romania

➡short description: ESign
ESign was the first created Certification Authority that offers PKI solutions. It enabled a communication and transaction of/between businesses and consumers over digital networks in a secure manner. ESign was the first to issue qualified certificates in accordance with the Law about electronic signatures.[665]
Being part of Verisign Trust Network guarantees that the certificates issued by E-Sign Romania meet the technical criteria for qualified certificates specified in Directive 1999/93/EC.

➡short description: Trans Sped Certification Authority
TransSped is issuing qualified certificates according to the EU Directive 1999/93/EU.[666]

Table 77 lists up all certification service providers in Romania:

Table 77: Certification Service Provider in Romania, source: own illustration

Certification Service Provider		Issued Certificates
National Trade Register Office		qualified certificates
ESign		qualified certificates
TransSped		n.a.

There is also a noncommercial Certification Authority in Romania. The IGCTI operates CAs for public services. It provides certification services to institutions of the central public administration.
Also the state telecommunication operator (the Special Telecommunication Service) hods certification authorities, serving some ministries, governmental agencies and the National Defense System.
Other Institutions. like bands or national companies have their own certification authorities, used in relation with the customer or for internal us.[667]

Inspecting authorities

The Ministry of Communication and Information Technology was notified as Supervisory and Regulatory Authority[668], exactly the Romania National Regulatory Authority for Communication and Information Technology ANRCTI.[669]

[665] cf. http://einvoices.idealsystems.gr/Adacom/Products_Services/PKI%20%20Authentication/Case%20Studies/ E_Sign.aspx, access on 09.08.07, 09:18

[666] cf. Correspondence with Viky Manaila, Managing Directror, Trans Sped SRL, Romania

[667] cf. http://www.igcti.ro/, access on 05.12.2007, 20:14

[668] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[669] cf. Correspondence with Viky Manaila, Managing Directror, Trans Sped SRL, Romania

2.22.3 Technical preconditions

Signature Software

The Banca Comerciala Romana, the Romanian Commercial Bank, provides a lo t of services, including money transfer, loan facilities etc, and invested in the development of an online solution for all its processes. They wanted to provide the ability to customers to digitally sign information, they submit through theses online-services. The Banca Comerciala Romana decided to implement a product, supplied by E-Lock: the FormSeal. Through this solution that can be integrated into any application customers are enabled to digitally sign and authenticate information and data. Also the bank is able to verify the authentication of sent documents. [670]

Also the Romanian ministry for communication and information technology is supplied by an electronic signature solution by E-Lock. DeskSeal, the solution method developed by E-Lock, enables to sign documents and data electronically and to encrypt them. By using digital certificates, users can be electronically identified and data can be saved and secured.[671]

Types of secure signature-creation device

➡Electronic ID card:

In Romania an electronic ID card is implemented to identify the user of online governmental services, where an authentication of the identify must me effected.

The digital signature that can be created by the ID card enables a secure access to information and online-services that are offered by public and private agencies. Thus, the validity of electronic transmitted document can be proofed.[672]

The STFD - TRANSFOND S.A. system for the domestic bank community as well as the system used by the Insurance Supervisory Commission rely on authentication by qualified signature. The signatures are based on electronic certificates that are installed on a secure USB token.

The ROVINARI system of the National Energy Faciliy Rovinari relies on advanced electronic signatures based on certifcates on secure USB tokens.[673]

TransSped is issuing qualified certificates on cryptographic smartcards or tokens, for example Gemalto (http://www.gemalto.com) or Cryptoflex eGate (http://www.cryptoflex.com/).[674]

---

[670] cf. http://www.elock.com/bank-romania.html, access on 25.07.2007, 18:29

[671] cf. http://www.elock.com, access on 25.07.2007, 18:29

[672] cf. Government of Romania, Ministry of Public Administration – the Government's strategy concerning the National Action Plan, e-Administration, Bucharest – 2001

[673] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Romania, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[674] cf. Correspondence with Viky Manaila, Managing Directror, Trans Sped SRL, Romania

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

In Romania, CRLs, OCSPs and LDAPs are used for electronic certificate validation.[675]

A list with revoked certificates can be found on the TransSped homepage as well as an OCSP service.[676]

2.22.4 Summary

Table 78 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 78: Summary and rating, Romania, source: own illustration

categories		rating
legal framework	The EU directive has been implemented in 2001.	A
technical standard	eGovl,eTax, eProcurement, eBanking all types of eS qualified certificates (HW, SW) USB token 5 CSP ID card, smartcards, token CRL and OCSP service, LDAP	A
distribution	Since April 2005, about 45.000 tax declarations have been sent via the National Electronic System SEN, signed with electronic signature based on qualified certificates (only software certificates) The eProcurement platform requires signatures for the usage. Since 2003, about 700 public institutions are interaction in the portal, and 700 private companies are suppliers. On the STFD system, about 10.000 signatures are used for inter-banking money transfers per day. Within Rovinari, employees use advanced eS on USB token to use the system and sign documents. Per day, 1.200 signatures are effected. Up to now, the CSP TransSped has issued about 8.000 certificates.	B

[675] cf. http://www.anrcti.ro, access on 05.12.2007, 20:27

[676] cf. https://ca.transsped.ro/repository/tscp.pdf, access on 25.07.07, 19:31

2.23 Slovakia

Figure 78: Fact-sheet: Slovakia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:53

In figure 78 some basic demographic and geographic data of the country is presented.

2.23.1 Institutional frame

Legislation

The EU Directive 1999/93/EC on a Community framework for electronic signatures was partially implemented by passing the Act No. 215/2002 on Electronic Signature (see Appendix – Slovakia: Act on Electronic Signature)and is becoming integrated onwards.[677]

In this act, there is also mentioned, that evidence that is signed electronically will be accepted in the court of justice. But this regulation is very complicated and strict. The Government is to prepare an amendment of that act to make it more practicable.[678]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Slovakia: National Regulations Details.[679]

[677] cf. Correspondence with Ivan Goldschmidt, Head of Chancellery, National Security Authority, Bratislava

[678] cf. Correspondence with Mag. Konstantin Bekos, commercial attaché for Slovakia, Federal Economic Chamber, foreign trade office Pressburg

[679] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Availability of Online Services

•eTax:[680]

In Slovakia, an eGovernment was implemented and e-public services are provided for citizens and businesses. These services enables, for example, the possibility to send the tax declaration electronically to the tax authority. The portal eTax is accessible at http://www.drsrsk. The system serves as communication system between citizens and enterprises and the tax authorities and tax documents can be delivered electronically to the tax authorities.

The system requires the use of qualified signatures based on qualified certificates, but also simple electronic signature with PIN code can be used.

In 2005, only 936 tax declarations have been filled electronically, thereof about 50 forms signed by qualified signatures.

•eVO (eTendering) - eProcurement:[681]

The electronic public procurement system is currently in implementing process It is an communication and information system for contact administration and was developed for contraction authorities and tenderers (natural and legal persons). The system enables tender submitting and accepting of tenderer proposals (eTendering). The system is accessible at http://www.evo.gov.sk for candidates and at http://www.evo.gov.sk/evo/ethics.nsf/homepage for contracting authorities.

The responsible organization is the Public Procurement Office.

•EKR - electronic communication system:[682]

Since 2005, the electronic communications interface EKR is operational and was developed for Slovak importers and traders. The system enables to send and receive transit and customs documents electronically and ensures a secure communications with the Slovak Customs Administration. The responsible organization is the Customs Directorate of the Slovak Republic.

The system requires advanced electronic signature on smartcards, USB token or based on software certificates. Furthermore, the documents are provided with timestamps.

Actually about 30.000 documents are signed and transmitted per month.

•other eServices:

All operational and planned eGovernment applications are summed up in the Appendix - Slovakia: Operational and planned applications.[683]

---

[680] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovakia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[681] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovakia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[682] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovakia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[683] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Types of electronic signature

In the Slovak Republic there are used advanced electronic signature and qualified electronic signature.

Qualified Electronic Signature is based on Qualified Certificates with the use of secure signature creation device pursuant to Directive 1999/93/EC Article 5.1.[684]

There are only few organizations that use electronic signature.[685]

The VUB Bank in Slovakia uses electronic signature as a security element to confirm a transaction (money transfer). The client is issued two customer certificates: a signing certificate and an encryption certificate. The client also gets s a private signing key to create an electronic signature and a public key for encryption. The Keys along with both certificates are saved either on a diskette or a chip card.[686]

The eVO eTendering system (currently in implementation phase) requires advanced electronic signature based on software certificates. Currently, no qualified electronic signatures are supported but are planned in the future.[687]

The eTax system relies on qualified electronic signatures based on qualified certificates or uses simple electronic signature with PIN codes. But in 2005, only 936 declarations have been transmitted electronically, only 50 thereof have been signed with qualified electronic signatures.[688]

The EKR system requires advanced electronic signature on smartcards, USB token or based on software certificates. Furthermore, the electronic documents are provided with timestamps.[689]

2.23.2 Application requirements

Types of certificates

In the Slovak Republic there exist Certificates and Qualified Certificates in accordance with Directive 1999/93/EC.[690]

---

[684] cf. Correspondence with Ivan Goldschmidt, Head of Chancellery, National Security Authority, Bratislava

[685] cf. Correspondence with Mag. Konstantin Bekos, commercial attaché for Slovakia, Federal Economic Chamber, foreign trade office Pressburg

[686] cf. http://www.vub.sk/en/show.asp?category=1953, access on 10.08.07, 19:08

[687] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovakia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[688] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovakia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[689] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovakia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[690] cf. Correspondence with Ivan Goldschmidt, Head of Chancellery, National Security Authority, Bratislava

The eVO eTendering system (currently in implementation phase) requires advanced electronic signature based on software certificates. The certificates for the system are generated and managed directly by the eVO system and issued after registration for the concrete tender.[691]

The eTax system requires qualified electronic signature based on qualified certificates on smart cards or USB tokens.[692]

The EKR system requires advanced electronic signature on smartcards, USB token or based on software certificates. Furthermore, the documents are provided with timestamps.

Certification Service Providers

In the Slovak Republic there are registered 9 Certification Authorities (CA) and 6 Accredited Certification Authorities (ACA) so far.[693]

Table 79 and table 80 sum all certification service providers in Slovakia:

Table 79: CA List, source: http://www.nbusr.sk/en/electronic-signature/ca-list/index.html, access on 13.08.2007, 08:53

Registration Number	Certification Authority	Residence	web address	beginning activity	notice
CA-001/2002	First Slovak Certification Authority (PSCA)	Borská 6, 841 04 Bratislava	www.psca.sk	1st May 2003	
CA-103/2003	Certification Authority VÚB (CA VÚB)	Mlynské nivy 1, 829 90 Bratislava 25	www.vub.sk	15th February 2003	Only for bank's clients!
CA-104/2003	Certification Authority EVPÚ (CA EVPÚ)	Trenčianska 19, 018 51 Nová Dubnica	www.caevpu.sk	2nd June 2003	
CA-206/2004	Certification Authority Dexia Slovakia	Hodžova 11, 010 11 Žilina	www.dexia.sk	1st December 2004	Only for bank's clients!
CA-307/2005	Certification Authority Apollo (CA APOLLO)	M.Čulena 5, 810 11 Bratislava 111	www.apollo.sk	15th June 2005	Only for insurance's clients!
CA-408/2006	Certification Authority Tedis	Bárdošova 2, 831 01 Bratislava	www.tedis.sk	16th January 2006	Only for contractual partners!
CA-409/2006	Certification Authority Disig CA Disig	Zahradnícka 151, 821 08 Bratislava	www.disig.sk	1st April 2006	Only for contractual partners!
CA-410/2006	První certifikační autorita, a.s.	Podvinný mlýn 2178/6 190 00, Praha 9	www.ica.cz	21st September 2006	
CA-511/2007	Certifikačná autorita Slovanet, a.s. (CA Slovanet)	Zahradnícka 151, 821 08, Bratislava	www.slovanet.sk	12th April 2007	Only for contractual partners!

[691] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovakia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[692] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovakia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[693] cf. Correspondence with Ivan Goldschmidt, Head of Chancellery, National Security Authority, Bratislava

Table 80: ACA List, source: http://www.nbusr.sk/en/electronic-signature/aca-list/index.html, access on 13.08.2007, 08:53

Registration Number	Accredited Certification Authority	Residence	web address	date of accreditation	Public Key Certificate (DER)
ACA-001/2004	CA EVPÚ	Trenčianska 19, 018 51 Nová Dubnica Slovakia	www.caevpu.sk	30th January 2004	09.02.2004 09.06.2005 04.11.2005
ACA-003/2004	Prvá slovenská certifikačná autorita (PSCA)	Borská 6, 841 04 Bratislava Slovakia	www.psca.sk	15th June 2005	27.07.2005
ACA-104/2005	The Slovak National Certification Authority (SNCA)	Budatínska 30, 850 07 Bratislava 57 Slovakia	ep.nbusr.sk/snca	15th August 2006	24.08.2006
ACA-205/2006	První certifikační autorita, a.s.	Podvinný mlýn 2178/6 190 00 Praha 9 Czech republic	www.ica.cz	21st September 2006	12.10.2006
ACA-206/2006	Certifikačná autorita Ministerstva obrany SR (CAMOSR)	Olbrachtova 5, 911 01 Trenčín Slovakia	www.pki.mil.sk (internal)	31st October 2006	19.12.2006
ACA-307/2007	Certification Authority CA Disig	Záhradnícka 151, 821 08 Bratislava 2Slovakis	www.disig.sk	26th July 2007	

The Ministry of Transport, Post and Telecommunications plans to implement about 1 000 eSignature „Contact Points“ by 2007, where citizens, that own an eSignature card can send electronically signed documents to public administrations.[694]

Inspecting authorities

The Slovak NSA is the central body of the state administration for the Electronic Signature and it is also a supervisory and accreditation body for Electronic Signature.

[694] cf. http://ec.europa.eu/idabc/en/document/6129/411, access on 27.06.07, 12:07

2.23.3 Technical preconditions

Signature Software

VUB is implementing electronic signature to secure electronic transactions, by signing and encrypting transmitted documents. VUB is also offering a program called „Encrypted mail explorer", that was developed for encrypting, reading and verifying mails. The program can be downloaded from the VUB homepage.[695]

In 2006, the Ardaco Company was founded. One of its products is QSign, a tool for protecting electronic documents. The Product works with documents in Microsoft Windows as an universal tool for text and graphic editors. QSign is an easy method for creating and verifying qualified electronic signatures. The application QSign was certified by the Slovakian National Security Authority.[696]

Types of secure signature-creation device

A list of secure certified products is on the web site of the NSA (table 81). The choice of a particular product is your decision.[697]

Table 81: Secure Signature Creation Device certified products, source: http://www.nbusr.sk/en/electronic-signature/products-certification-for-qualified-electronic-signature/list-of-certificated-products/certificated-products-for-qualified-electronic-signature-users/index.html, access on 13.08.2007, 08:54

Product	Producer	Period of certificate validity	Characteristics
Cryptoflex 32K e-Gate Smart Card by SchlumbergerSema	SchlumbergerSema	to 8th September 2007	Multi-purpose SSCD with SSCD application QSign personalization for Qualified Electronic Signature use
Chip Card Siemens HiPath Slcurity Smart Card 32KB, verzia CardOS 4.3B	Chip SLE66CX322P Infineon Technologies AG, Mníchov, Nemecko OS CardOS 4.3B Siemens AG, Mníchov, Nemecko	to 24th November 2008	Single -purpose SSCD/ for Multi-purpose SSCD, application SigG must be used for Qualified Electronic Signature
Chip Card Siemens HiPath Sicurity Smart Card 64KB, verzia CardOS 4.3B	Chip SLE66CX642P Infineon Technologies AG, Mníchov, Nemecko OS CardOS 4.3B Siemens AG, Mníchov, Nemecko	to 6th December 2008	Single -purpose SSCD/ for Multi-purpose SSCD, application SigG must be used for Qualified Electronic Signature
USB produkt „iKey 2032", Hardware version A, Firmware version 0.6	SafeNet, Inc.	to 31st January 2009	Single -purpose SSCD

[695] cf. http://www.vub.sk/en/show.asp?category=1953 , access on 10.08.07, 19:08

[696] cf. http://www.ardaco.com, access on 27.06.07, 12:19

[697] cf. Correspondence with Ivan Goldschmidt, Head of Chancellery, National Security Authority, Bratislava

Product	Producer	Period of certificate validity	Characteristics
Chip Card STARCOS SPK 2.3	Chip P8WE5032V0G: Philips Semiconductors Hamburg Unternehmensbereich der Philips GmbH, OS STARCOS SPK2.3: Giesecke & Devrient GmbH, Prinzregentenstraße 159, D-81607 München, Germany	to 31st January 2009	Single -purpose SSCD
Safenet iKey 2032 FIPS Hardware versions (A and 909-23002) and 909-25001 Firmware version 0.6	SafeNet, Inc.	to 31st March 2009	Single -purpose SSCD

Products for Signature Creation and Verification Applications, recommended by the NSA, can be found on the homepage of NSA (tables 82-85).

Table 82: Secure Signature Creation Device for qualified electronic signature users, recommended by the NSA, source: http://www.nbusr.sk/en/electronic-signature/products-certification-for-qualified-electronic-signature/products-list-in-the-certification-process/products-for-qualified-electronic-signature-users/index.html, access on 13.08.2007, 08:55

Product	Producer	supposed finishing of a certification process
CryptoPlus/SSCD, version 1.9	Monet +, a.s., Zámecká 365, 763 14 Zlín Czech Republic	30th September 2007
ePass2000	Gratex International a.s. Plynárenská 7/C 821 09 Bratislava Slovakia	Applicant have not delivered complete documentation to certification process

Table 83: Signature Creation and Verification Application for qualified electronic signature users, recommended by the NSA, source: http://www.nbusr.sk/en/electronic-signature/products-certification-for-qualified-electronic-signature/products-list-in-the-certification-process/products-for-qualified-electronic-signature-users/index.html, access on 13.08.2007, 08:55

Product	Producer	supposed finishing of a certification process
Signer, version 3.0	PVT PROKOM, a.s. Kovanecká 30/2124 190 00 Praha 9 – Libeň Czech Republic	Applicant have not delivered complete documentation to certification process
SigMan, version 1.8	PVT PROKOM, a.s. Kovanecká 30/2124 190 00 Praha 9 - Libeň Czech Republic	Applicant have not delivered complete documentation to certification process

Table 84: Software for Trustworthy System for CSP, recommended by the NSA, source: http://www.nbusr.sk/en/electronic-signature/products-certification-for-qualified-electronic-signature/products-list-in-the-certification-process/products-for-certification-service-providers/index.html, access on 13.08.2007, 08:55

Product	Producer	supposed finishing of a certification process
UniCERT version 5.2.1.900	Cybertrust	30th September 2007

Table 85: Signature Creation Application and Signature Verification Application, recommended by NSA, source: http://www.nbusr.sk/en/electronic-signature/products-certification-for-qualified-electronic-signature/list-of-certificated-products/certificated-products-for-qualified-electronic-signature-users/index.html, access on 14.08.2007, 08:57

Product	Producer	period of certificate validity	Characteristics
QSign version 1.37	Infotrust a.s. Bratislava, NBÚ Bratislava	to 11th November 2008	SCVA CAdES-EPES CAdES-EPES-T CAdES-EPES-C-X CAdES-EPES-A Archival Signature
QSign - Aplikácia pre ZEP, version 2.0	Infotrust a.s. Bratislava	to 23rd February 2009	SCVA CAdES-EPES CAdES-EPES-T CAdES-EPES-C-X CAdES-EPES-A Archival Signature
QSign version 3.0	Ardaco, a.s., Slovinec 41, 841 07 Bratislava NBÚ SR	to 11th October 2009	SCVA CAdES-EPES CAdES-EPES-T CAdES-EPES-C-X CAdES-EPES-A Archival Signature
ZEP-Entelligence version 1.3	TEMPEST, a.s., Plynárenská 7/B, 821 09 Bratislava	to 17th March 2009	SCVA XAdES-EPES XAdES-EPES-T
ZEP Sign Center, version 1.1 r2	Softip, a.s., Spojová 21, 974 01 Banská Bystrica Slovakia	to 01st January 2008	SCVA XAdES-EPES XAdES-EPES-T
ZEP- XML, version 2.0	TEMPEST, a.s., Plynárenská 7/B, 821 09 Bratislava, Slovakia	to 31st March 2009	SCVA XAdES-EPES XAdES-EPES-T
D. Signer/XML version 1.0.0.5	Ditec, a.s., Plynárenská 7/C, 821 09 Bratislava Slovakia	to 31st December 2007	SCA ZEP XML
D. Signer/PDF version 1.0.0.0	Ditec, a.s., Plynárenská 7/C, 821 09 Bratislava Slovakia	to 31st December 2007	SCA ZEP-XMLSig verzia 1.0

Product	Producer	period of certificate validity	Characteristics
QSign version 3.1	Ardaco, a.s., Polianky 5 841 01 Bratislava Slovakia	to 1st August 2010	SCVA CAdES-EPES CAdES-EPES-T CAdES-EPES-C-X CAdES-EPES-A Archival Signature

Card readers

Smart card readers must cooperate with certified Secure Signature Creation Devices.[698]

Certificate requirements

n.a.

Application programming interface for online-verification

An CRL is mandatory for the Certification Service Provider.[699]

2.23.4 Summary

Table 86 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 86: Summary and rating, Slovakia, source: own illustration

categories		rating
legal framework	The EU directive was only partially implemented in 2002. Electronically signed documents are accepted in the court, but the regulation is very complicated and strict. To make it more practicable, an amendment is prepared.	B
technical standard	eGovernment, eTax advanced and qualified electronic signature, qualified certificates (HW, SW) 9 CA and 6 accredited CA CRL	A
distribution	eTax: in 2005, only 936 tax declarations have been filled electronically, about 50 forms singed by qualified eS There are only few organizations that use ES. VUB Bank uses ES for confirming transactions of its clients. The Ministry of Transport, Post and Telecommunication plans to implement “1000eSignature Contact Points” by 2007.	C

[698] cf. Correspondence with Ivan Goldschmidt, Head of Chancellery, National Security Authority, Bratislava

[699] cf. Correspondence with Ivan Goldschmidt, Head of Chancellery, National Security Authority, Bratislava

2.24 Slovenia

Figure 79: Fact-sheet: Slovenia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 79 some basic demographic and geographic data of the country is presented.

2.24.1 Institutional frame

Legislation

On the 1st september of 2000, the Electronic Commerce and Electronic Signature Act became effective (see Appendix - Slovenia: ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE ACT). Further, the decree on electronic commerce and electronic signature was issued (see Appendix - Slovenia: Decree on Conditions for Electronic Commerce and Electronic Signing).[700]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Slovenia: National Regulations Details.[701]

Availability of Online Services

•eGovernment:

In March 2001, Slovenia launched a eGovernment Portal e-Uprava, relaunched it in December 2003 and

[700] cf. Correspondence with Mag. Christian Miller, commercial attaché for Slovenia and Albania, Federal Economic Chamber, foreign trade office Ljubljana

[701] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

modernised it in May 2006- The portal is found under http://e-uprava.gob.si/ (figure 80). It provides access to administrativer forms that can be handled full electronically.[702]

Figure 80: eGovernment Portal Slovenia, source: http://e-uprava.gov.si/, access on 10.12.2007, 19:13

• eDavki - eTax system:

Since 2004, individuals and companies can file their taxes online by filling-out an online form, validate data and digital sign and timestamp it. The system can be accessed at http://edavki.durs.si (figure 81).

The eTax system of Slovenia is a combination of a web portal and a back office on the highest level of security. The portal connects with governmental institutions and exchanges information. All procedures are based on qualified certificates that enable authentication and the digital signature.[703]

The system relies on the PKI framework that is widely used in the country.

The tax payers sign the forms electronically and the Tax Administration verifies the signed data by connection to the certification authority that has issued the certificate.[704]

[702] cf. European Commission, eGovernment Factsheet - Slovenia - National Infrastructure, 14.December 2007, http://www.epractice.eu/document/3474, access on 04.12.2007, 17:08

[703] cf. European Commission, eGovernment Factsheet - Slovenia - National Infrastructure, 14.December 2007, http://www.epractice.eu/document/3474, access on 04.12.2007, 17:08

[704] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Figure 81: eTax Portal eDavki, source: http://edavki.durs.si/, access on 10.12.2007, 19:15

Most people use software certificates for authentication, some use smartcards. Government employees mostly use their smartcards, also for filling forms for personal income declaration electronically.
The responsible organizations are the Ministry of Finance and the Tax Administration.
The eTax system is currently used by 43.614 registered users. The number of registered certificates is 52.604 and in 2006, 273.959 documents have been deposited.[705]

•e-SJU - eService Portal of the public administration:[706]
This portal offers different forms and services of life events on a single platform. Any public institution and administration can use the portal for publishing its forms by using digital signatures. The portal can be accessed at http://e-uprava.gov.si/storitve (figure 82).
The responsible organization is the Ministry of Public Administration.

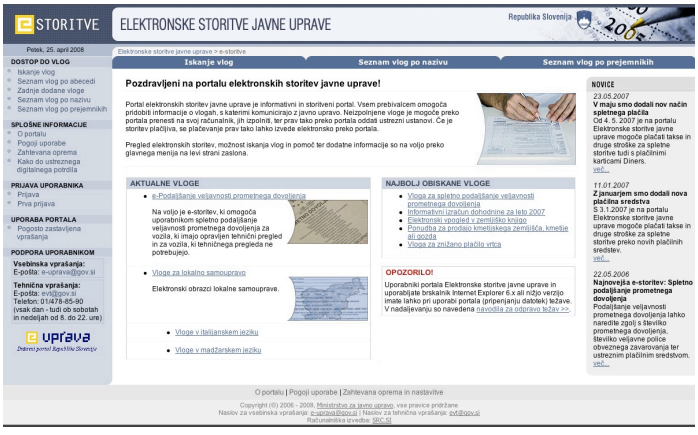


Figure 82: e-SJU Portal, source: http://e-uprava.gov.si/storitve/, access on 10.12.2007, 19:19

[705] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[706] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

The portal requires the use of qualified signature based on qualified certificates for some forms.
The citizen or companies that visit the portal must sign the forms in pdf format and the Ministry of Public Administration verifies the data and provides timestamps, public institutions receive and use the signed data for further handling. For verifying a signature, the system connects to the certification service provider that issued the certificate and stores the verified data at the portal side.
The signatures rely on the PKI framework that is widely used in Slovenia.
Most people use their software certificates for authentication and signature features, in some cases also smartcards are used.
Detailed statistics on the current use of electronic signatures are not available yet.[707]

•EPOS - Information system of Slovene Customs:[708]
This system is in the testing phase and shall support the collection and control of different customs declarations enabling online communications between all institutions that are participating like accredited companies, reporting units and companies offering commercial programming tools to report customs data. The system supports the acceptance of declarations, verifies electronically signed messages and direct them to the dedicated application.
Each user must register to use this application. Legal persons report customs data and sign them electronically, also the Customs Administration prepare and sign documents they received (paper declarations), the Cusoms Administration verifies the signed data and sign return messages. The System relies on qualified XML signatures (W3C XML Signatures) that are based on qualified certificates.
The responsible organizations are the Ministry of Finance and the Customs Administration.
Most users use their software certificates for authentication and signature features, some use smartcards.
The use of tokens and smart cards is strongly encouraged, the Customs Administration employees have their certificates already on smart cards.
There is no statistic on the use of electronic signatures available yet.

•Registration Authority Application:[709]
This application aims to support all procedures for issuing and managing certificates obtained from the certification service provider SIGEN-CA. This system is accessible for Registration Authority staff and supports the procedures of issuance, revocation and recovery of certificates. If a user wants to fill a form, he goes to the registration authority (like consulates or the tax office), the clerk enters all data using this application and digitally signs the form using a certificate issued by SIGOV-CA. SIGEN-CA and SIGOV-CA both belong to the Trust Service Provider at MPA, the Ministry of Public Administration. The responsible organization is the Ministry of Public Administration.
The application requires the use of qualified signatures based on qualified certificates that are issued by SIGEN-CA and SIGOV-CA.
The first modules of this application are operating since December 2001. A Web portal is under

[707] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[708] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[709] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

development where certificate holders can fill forms directly on the web interface.
Since 2001, about 38.000 signatures have been used in the module for natural persons, about 10.000 in the module for legal persons.

•Intrastat - Collecting and controlling system for Intrastat data:[710]
This system supports the collection and control of Intrastat data in the sector of foreign trade. The Application is used by companies that are registered within the Eurpean Union and are accredited for reporting data for Slovene companies. The system is accessible at http://intrastat-surs.gov.si.
Each user must register to use this application. Companies register at the Customs Administration and possess a qualified certificate for authentication. Currently the system does not sue digital signatures.
The responsible organization is the Statistical Office of Slovenia.

•„One-Stop-Shop“ - State Portal for Businesses:[711]
Since July 2005, a state portal for businesses is operating. It enables natural persons to register their business activity in the Register. Most of the procedures for filling forms require digital signature. The use of qualified certificates is supported. The Ministry of Public Administration verifies the signed data.
Most people use software certificates, some use smartcards.
Since July 2005, 32.569 forms have been digitally signed.

•other ePortals

The Certification Service Provider HalcomCA issues different kinds of certificates for different purposes. These certificates also serve as entry into secure electronic business through different portals in Slovenia (table 87[712]).[713]

Table 87: ePortals in Slovenia, source: own illustration

Target group	ePortals in Slovenia		Website
legal entities	AJPES	AJPES	http://www.ajpes.si/
	Banka Celje	banka celje	http://www.banka-celje.si/
	Custom Administration of the Republic of Slovenia	Ministry of Finance Customs Administration of the Republic of Slovenia	http://www.carina.gov.si/en/
	DBS PRONET (Deželna banka Slovenije)	DEŽELNA BANKA SLOVENIJE	http://www.dbs.si/podjetja/elektronska-poslovalnica.html
	eDavki	eDavki	http://edavki.durs.si/
	E-storitve	E-STORITVE	http://e-uprava.gov.si/storitve/
	E-uprava	uprava	http://euprava.gov.si/e-uprava/euprava.euprava
	E-zaposlitve	uprava	http://e-uprava.gov.si/ez/
	INTRASTAT	INTRASTAT	http://intrastat-surs.gov.si/

[710] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[711] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[712] cf. http://wwweng.halcom-ca.si/index.php?section=18, access on 28.11.2007:13:13

[713] cf. Correspondence with Luka Ribicic, Halcom CA, Slovenia

Target group	ePortals in Slovenia		Website
	KDD		http://www.kdd.si/
	Net.Stik (Sparkasse)		http://www.sparkasse.si/
	Poslovni Bank@Net (NKBM)		http://www.nkbm.si/defaulteng.aspx/
Individuals	Abanet		http://www.abanka.si/
	eDohodnina		http://edavki.durs.si/OpenPortal/
	E-storitve		http://e-uprava.gov.si/storitve/
	e-VEM		http://evem.gov.si/sp/
	E-zaposlitve		http://e-uprava.gov.si/ez/
	Mobitelov spletni Monitor		https://monitor.mobitel.si/selfcarenew/login.html

•other eServices:

There are a lot more electronic services, using qualified XML signatures based on qualified certificates, like the system for annual reports (since 2003, for business entities, 9721 users), Financial Accounts Statistics (since 2004, for bigger companies ,2375 users), system for Salary Reporting (since 2005, for business entities, 4.094 users) etc.

Other systems are in development phase, like a system for waste management (in development) or for online access to health insurance data (rollout middle 2008).

All operational and planned eGovernment applications are summed up in the Appendix - Slovenia: Operational and planned applications.[714]

Types of electronic signature

The eTax system as well as the e-SJU portal and the EPOS system rely on the use of qualified signature based on qualified certificates.[715]

2.24.2 Application requirements

Types of certificates

The Slovenian Governmental Certification Authority Sigov-CA issues qualified digital certificates following all requirements regarding encryption in accordance with the Law. Those certificates are used by the public administration employees.

The Ministry of Public Administration CA issues four different digital certificates:

SIGOV-CA: - enterprise digital certificates
- web digital certificates

[714] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[715] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

SIGEN-CA: - enterprise digital certificates for legal and natural persons,
- web digital certificates for legal and natural persons.

Digital certificates are used in public administration and issued to employees and other that are associated to the institution. The SIGEN-CA certificates are issued to legal and natural persons to exchange data securely and legitimately with the public administration.[716]

There are other commercial certificates that are accepted, but they are not government sponsored and not accepted when dealing with official administration (like Postar CA issued by the Slovenian Post.)[717]

HalcomCA issues the following certificates:

- for legal entities:
- advanced qualified digital certificates
- mobile qualified digital certificate for individuals:
- standard qualified digital certificates
- advanced qualified digital certificates
- mobile qualified digital certificates
- time stamp:
  time stamping service.[718]

To date, Halcom CA has issued about 120.000 digital certificates for employees of different companies and banks[719] on smartcards in 7 markets.[720]

HalcomCA is the first certificate authority in the world that enables the access to multiple accounts at different banks in Slovenia and abroad with one digital certificate. The participating banks in Slovenia and abroad can be found at http://wwweng.halcom-ca.si/index.php?section=16 and http://wwweng.halcom-ca.si/index.php?section=17.

The Certification Service Provider HalcomCA issues different kinds of certificates for different purposes. These certificates also serve as entry into secure electronic business through different portals in Slovenia (see Chapter Slovenia - Availability of Online Services - ePortals).[721]

The eTax system as well as the e-SJU portal and the EPOS system require qualified signatures based on qualified certificates.[722]

---

[716] cf. Certification Authority, Ministry of Public Administration, Purpose of the CA, http://www.si-ca.si/eng/eng-namen.php, access on 10.12.2007, 19:24

[717] cf. Correspondence with Jan Jona Javorsek, SiGNET CA staff, Ljubljana, Slovenia

[718] cf. Halcom CA, Identity of certificate authority Halcom CA, http://wwweng.halcom-ca.si/index.php?section=14, access on 02DEZ08

[719] cf. http://wwweng.halcom-ca.si/, access on 10.12.2007, 19:32

[720] cf. Correspondence with Luka Ribicic, Halcom CA, Slovenia

[721] cf. Correspondence with Luka Ribicic, Halcom CA, Slovenia

[722] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Certification Service Providers

The governmental certificate service provider are the Slovenian Governmental Certification Authority Sigov-CA and the Slovenian General Certification Authority Sigen-CA by the Ministry of Public Administration.

➡Short description: Slovenian Governmental Certification Authority Sigov-CA

Since January 2001, SIGOV-CA is part of the Governmental Certification Authority that function as Trusted Third Party. It issues qualified digital certificates for employees and servers of public administration institutions.

➡Short description: Slovenian General Certification Authority Sigen-CA

Sigen-CA operates since July 2001 and issues qualified digital certificates for citizen and for legal and natural persons, registered for performing activities.

➡Short description: Slovenian Time Stamping Authority SI-TSA

The Slovenian Time Stamping Authority is part of the Certification Authority of the Ministry of Public Authority.

Also other not governmental supported certification service provider operate in Slovenia, but in the planned eID card project only the certificates of the governmental certification authorities are relevant.

➡Short description: Halcom d.d. CA

Halcom CA was founded in 1999 and is thus the oldest and largest certification authority in Slovenia. It provides the safest PKI technology on smart cards.[723]

Table 88 lists up all certification service providers in Slovenia.

Table 88: Certification Service Provider in Slovenia, source: own illustration

Certification Service Provider		Issued Certificates
SIGOV-CA	Certification Authority SIGOV-CA Ministry of Public Administration	qualified digital certificates for employees and servers of public administration
SIGEN-CA	Certification Authority SIGEN-CA Ministry of Public Administration	qualified digital certificates for natural and legal person
SI-TSA		trusted time stamps for application of public administration
Halcom CA	halcom CA Certificate Authority	advanced digital certificates for lega entities standard qualified digital certificates for individuals advanced qualified digital certificates of individuals Time Stamping
Post Slovenia	POŠTA SLOVENIJE	n.a.

[723] cf. Correspondence with Lika Ribicic, Halcom CA, Slovenia

Inspecting authorities

There is no accreditation authority in Slovenia, all registered certification service provider are supervised by the Ministry of Economy.

2.24.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

eID card project:

In February 2003, Slovenia has started to develop electronic identity cards. First, issuance was planned for 2005, but then postponed for at the least 3 years. The eID card is personalized and a combination of a conventual IDcard and a signature card. Qualified certificates will be stored on the card.[724]

The cards had not been introduced until April 2007. The Project is not expected to be rolled out again in 2008.[725]

Card readers

Halcom CA offers a range of smartcard readers together with necessary drivers on their homepage (figure 83). HalcomCA supports and recommends Omnikey and Towitoko.[726]

Reader type	Operation system			
	WIN 98/ME WIN 2000 WIN XP SP1	WIN XP SP2	WIN NT	WIN 2003 SERVER
CARDMAN 1010 OZ. OCR 136	✓	✓	✓	✓
CARDMAN 2020 OZ. OCR 150	✓	✓	-	✓
CARDMAN 3121	✓	✓	-	✓
CARDMAN 4000 OZ. OCR 101	✓	✓	✓	✓
CARDMAN 4040	✓	✓	✓	✓
TOWITOKO CHIPDRIVE (MICRO) 110 TOWITOKO CHIPDRIVE (MICRO) 120	✓	✓	-	-

Figure 83: Drivers for smartcard readers, offered by Halcom CA, source: http://wwweng.halcom-ca.si/index.php?section=30, access on 04.12.2008

[724] cf. Modinis - IDM, National Profile for eGovernment IDM Initiatives in Slovenia, http://ic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/SlovenianProfile , access on 10.12.2007, 19:37

[725] cf. European Commission, eGovernment Factsheet - Slovenia - National Infrastructure, 14.December 2007, http://www.epractice.eu/document/3474, access on 04.12.2007, 17:08

[726] cf. Correspondence with Luka Ribicic, Halcom CA, Slovenia
also see http://www.omnikey.com, http://www.towitoko.de

Certificate requirements

Within the EPOS system users must install an ActiveX web component to digitally sign messages.[727]

Application programming interface for online-verification

Halcom CA offers a revocation list on their homepage under http://wwweng.halcom-ca.si/index.php?section=29.

2.24.4 Summary

Table 89 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 89: Summary and rating, Slovenia, source: own illustration

categories		rating
legal framework	In 2000, the Electronic Signature Act became effective.	A
technical standard	eGov, eTax, lot of other ePortals and eServices basic, advanced, qualified certificates (SW, HW), mobile certificates Smartcards, 5 CSP ID card project under development CRL	A
distribution	the eTax system relies on PKI framework that is widely used, currently 43.614 registered users, 52.604 registered certificates. In 2006, 273.959 documents deposited. Registration Authority Application: since 2001, about 48.000 signatures have been used. Up to April 2007, about 120.000 digital certificates for employees of different companies and banks had been issued by Halcom CA.	A

[727] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Slovenia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

2.25 Spain

Figure 84: Fact-sheet: Spain, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 84 some basic demographic and geographic data of the country is presented.

2.25.1 Institutional frame

Legislation

The basic for electronic signatures was created by the law 59/2003 for electronic signature (see Appendix - Spain: LEY 59/2003, de 19 de diciembre, de firma electrónica, only available in Spanish).[728]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Spain: National Regulations Details.[729]

•recognition of foreign certificates:
recognition of foreign certificates:[730]
In March 1998, the agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:
Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

[728] cf. Correspondence with Mag. Friedrich Steinecker, commercial attaché for Spain, Federal Economic Chamber, foreign trade office Madrid

[729] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[730] cf. Study of the Donau Universität Krems, Master-Studie, Austria

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Spain was one of the founding members of the CCRA and has made important steps forwards. Its participatory status within the Common Criteria Mutual Recognition Agreement has changed from certificate consuming into certificate authorizing participant. The Spanish scheme has been approved to issue Common Criteria certificates for mutual recognition within the Recognition Agreement.[731]

Availability of Online Services

•eGovernment[732]

Spain is a very regional state with 17 autonomous communities that have different grade and speed of development of eGovernment applications.

Using electronic signature for eGovernment applications started a decade ago with the implementation of the electronic tax declaration system (see next point eTaxes).

In Spain, strong efforts are made concerning electronic information share. In the near future, all Administrative Bodies will share information electronically.

The Public Administration Ministry MAP coordinates all eGovernment applications at state level. All On-line services that are provided by State Administration is provided by www.060.es, some of them using digital certificates or not. The design of the portal is shown in figure 85.

Figure 85: State eGovernment www.060.es, source: http://www.060.es/, access on 11.12.2007, 09:03

[731] cf. Study of the Donau University Krems, Master-Study, Spain

[732] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

The 17 autonomous Communities have all their own Internet portals, offering information or linking to online transactions. Some of them already provide eGovernment services, requiring eSignatures or the use of eID cards. A detailed table about all Spanish Regions, the official portal and the provided eGovernment services can be seen in Appendix - Spain: Regional Government, official Portals and eGovernment applications.
Of the 17 regions, 12 provide eGovernment Services and use eSignature, 4 of them adapted the use of eID cards.

But also Spanish cities want to provide their services online. Thus, some have already implemented web portals including eSignature applications. Barcelona, Bilbao, Madrid and Valencia are working to extend their online offer, especially transactions like payment of taxes, issuing of certificates or standing orders.
The online transactions and webpages of the cities are listed at the following web sites:

- Barcelona's online transactions: http://w10.bcn.cat/APPS/STPSipacWeb/inici.do?i=e
- Bilbao municipality webpage: http://www.bilbao.net/nuevobilbao/jsp/bilbao/ciudad.jsp?idioma=C&color=rojo&padre=|HA&tema=|T|
- Madrid's online transactions: http://www.munimadrid.es/portal/site/munimadrid/menuitem.2366ae1c4f6e0b0aa7d2245f0191fc08a0c/?vgnextoid=66e39374bcaed010VgnVCM1000000b205a0aRCRD&vgnextchannel=f4683a940ed07010VgnVCM100000dc0ca8c0RCRD
- Valencia's municipality webpage: http://www.valencia.es/ayuntamiento2/ndportada.nsf/(Portadas1)/$first?opendocument&lang=1

One example of the offer of a municipality webpage is the site of Bilbao (figure 86).

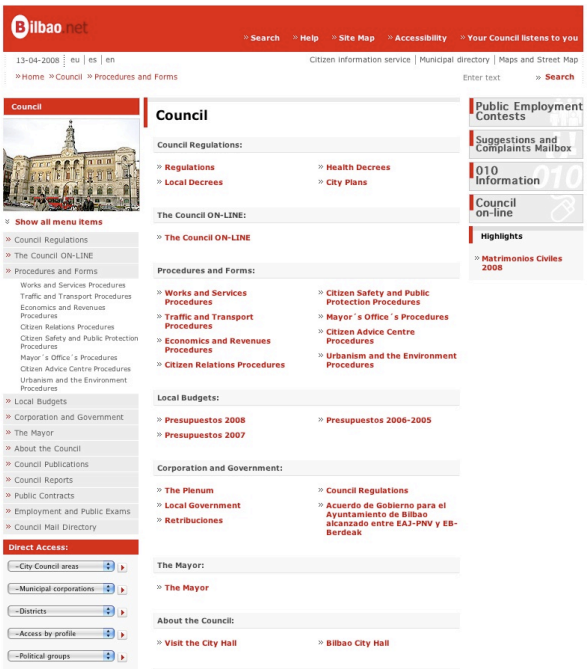


Figure 86: Bilbao's municipality webpage, source: http://www.bilbao.net/nuevobilbao/jsp/bilbao/ciudad.jsp?idioma=C&color=rojo&padre=|HA&tema=|T|, access on 11.12.2007, 09:08

But Spain is keen on improving and simplifying all electronic services and approved different initiatives to modernize the Administration. The authority that is in charge of eGovernment cooperation and coordination function is the Ministry of Public Administration.[733]

•eTaxes:[734]
Personal income taxes can be declared on-line via the application provided by the Tax Agency. It is possible to pay the tax e-signing the request and sending it to around 140 Financial Entities.
The Agencia Tributaria (AEAT) develops a program that runs on a local computer of the taxpayer and helps to calculate the data. More than 98% of the taxpayers use it. It delivers a file that can be sent via Internet to the server of the AEAT after digitally signing it; also it is possible to print it with a PDF-417 code that includes the same file with all the data of the form.
In order to help the filling of the income tax it is possible to download to the local computer all the relevant data that the AEAT knows.

Also it is possible to accept an income tax already prepared by AEAT, and even modify it and later accept it.

Is it possible to sign an income tax declaration for 2 persons, where each of them sign the same data.
3.783.784 annual income taxes were accepted via internet for fiscal year 2005..735
Also VAT taxes can be declared on-line via the application provided by the Tax Agency.
Declarations can be done using a commercial and noncommercial user certificate and the ID-card.

1.375.126 annual vat income taxes declarations and 1.989.693 periodical vat income taxes declarations were accepted via internet for fiscal year 2005.

Corporation taxes can be declared on-line via the application provided by the Tax Agency.

Declarations can be done using a commercial and noncommercial user certificate. There is no plan for an e-ID card for corporations, so they use smart cards and software certificates.

399.028 annual corporation tax declarations and 31.266 periodical corporation tax declarations were filed via internet in fiscal year 2005.

Withdrawal taxes on employees' income can be declared on-line via the application provided by the Tax Agency).
Declarations can be done using a commercial and noncommercial user certificate.
Declarations can be done using a commercial ca certificate, either by the employer himself, or through a mandated professional service provider.

650.986 periodical withdrawal taxes on employees' income declarations and 1.388.381 annual informative declarations were accepted via internet for fiscal year 2005.

---

[733] for more information see http://www.map.es

[734] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

[735] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

•Registro Telematico - online Registry:[736]
At Registro Telematico, citizens can present and submit any request to the Ministry of Education and Science. Also complaints to judicial means as well as appeals for judicial review are presented and available online. The registry is accessible at http://www.mec.es/mecd/registro and relies on advanced electronic signatures that are issued by FNMT Royal Mint, stored on smartcards or based on software certificates.
The first version of the system was launched in January 2005, the second version in November 2005. In 2006, about 300 users accessed the applications.

•Application delta:[737]
The Systm Delt@ for the employment sector manages all work flow that is related to labour accidents. The system requires advanced electronic signatures most of them based on qualified software certificates. Every year, about 2.000.000 signed documents are transmitted.

•Avanz@ - Profit - Politica Industrial TIC[738]
Avanz@ is an system that provides aids for R&D Investments, Information Society Services and the industrial sector with the aim to achieve market growth in ICT sector and in the use of IT. It can be accessed via http://www.mityc.es/profitTIC. The system involves all procedures that are related to the cycle of aid concession and requires the use of advanced electronic signatures and allows the creation of qualified signatures by using the eID card.
Per year about 1.500 users with electronic signature use the system per year.

•LexNet . eJustice system:[739]
This system was developed the Justice sector for public officers of Judiciary organs, Public Prosecutors, Lawyers, Solicitors, legal representatives and organs and institutions of the State Administration. The system enables secure delivery of notifications and informations via email.
Currently, the system is under development and operating only in some regions.
The responsible organization is the Ministry of Justice.
LexNet requires the use of qualified signatures on smart cards.
Up to now, about 150.000 notifications have been transmitted. But the application has to face some barriers, in some cases legal difficulties.

---

[736] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[737] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[738] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[739] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•other eServices:[740]
All operational and planned eGovernment applications are listed up in the Appendix - Spain: Operational and planned applications.

Types of electronic signature
There are two kinds of electronic signature:

- signature that is enabled by an e-ID card (for natural persons) or
- advanced signature with an user certificate.[741]

According to the law, tree types of signatures are defined:

- firma electrónica (electronic signature): collection data in electronic form, associated or attached to other electronic data, possibility to identify the signatory
- firma electrónica avanzada (advanced electronic signature): identification of signatory, uniquely linked to signatory, under sole control of signatory, detects all changes of signed data
- firma electrónica reconocida (recognized electronic signature): equivalent to qualified electronic signature in the European Directive, advanced electronic signature based on recognized certificated, generated by secure creation device, same value as handwritten signature.[742]

The system Registro Telematico, is accessible at http://www.mec.es/mecd/registro and relies on advanced electronic signatures that are issued by FNMT Royal Mint, stored on smartcards or based on software certificates.
The Systm Delt@ for the employment sector requires advanced electronic signatures most of them based on qualified software certificates.
Avanz@ requires the use of advanced electronic signatures and allows the creation of qualified signatures by using the eID card.
LexNet (under development and operating only in some regions) requires the use of qualified signatures on smart cards.[743]

[740] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[741] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

[742] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[743] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

2.25.2 Application requirements

Types of certificates

Certificates can reside at a smart card or be a software certificate.[744]

Spain issues eID cards since March 2006. The eID card fulfills two different functions: Authentication and signature. Therefore it stores three electronic certificates:

- the component certificate to authenticate the eID and establish an encrypted channels between card and drivers
- the authenticate certificate that guarantees the citizen‘s identity
- the signature certificate to sign documents electronically and guarantees the integrity and non-reputation of the document.

The fields of signature certificates is described in the Appendix - Spain: Fields of the signature certificate in detail.[745]

The certificates are for all natural person and institution that have a NIF (Spanish Identification Number) and have registered after a physical identification and documentation of legal representation. The certificate for an institution has always the identification of a natural person as its representative.[746]

Most people use Software Certificates, only few use the ID card and other certificates on smart cards.

Until now there is no interoperability with certificates issued in other countries because they don’t have the Identification Number, at least, at the OID where it is expected.[747]

Actually, the certification service provider FNMT Ceres has issued 1.654.556 certificates.[748]

Certification Service Providers

There are around 15 accredited certification authorities in Spain.[749]

The Ministry of Public Administration provides a multiPKI Validation Platform that provides validation of electronic certificates and electronic signatures of the recognized certification authorities to eGovernment

---

[744] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

[745] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[746] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

[747] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

[748] cf. Correspondence with Cristina Acedo, Ceres, FNMT - RCM, Spain

[749] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

applications. This Platform holds 12 CSP and 56 types of electronic certificates. a detailed list is shown at http://www.dnielectronico.es/seccion_aapp/rel_autoridades.html.[750]

Table 90 lists up all certification service providers in Spain:

Table 90: Main Certification Service Providers in Spain, source: own illustration

	Certification Service Providers		Web page	issued certificates
Public Providers	DGP (Dirección General de la Policía)		http://www.dnielectronico.es/	n.a.
	FNMT-CERES (Fábrica Nacional de Moneda y Timbre)		http://www.cert.fnmt.es/	qualified electronic signatures
	CATCert (Agència Catalana de Certificació)		http://www.catcert.net/web/cat/inici/home.jsp	n.a.
	ACCV (Autoritat de Certificació de la Comunitat Valenciana)		http://www.accv.es/default_default.htm	n.a.
	IZENPE		http://www.izenpe.com/s15-5218/es/	n.a.
Private Providers	AC Camerfirma		http://www.camerfirma.com/	digital certificates to cooperate persons or entities
	ANF AC (Asociación Nacional de Fabricantes - Autoridad de Certificación)		http://www.tradise.com/tradise/	digital certificates for natural persons digital certificates for corporate persons or entities
	ANCERT (Agencia Notarial de Certificación)		http://www.ancert.com/	digital certificate for notary personal and corporate persons and entitis, digital certificates for public corporations, digital certificates for employes
	Firma Profesional		http://www.firmaprofesional.com/bienvenida.htm	digital certificates with enrollment in professional bodies
	ACA (Autoridad de Certificación de la Abogacía)		http://www.cgae.es/especial/acaredabogacia/acaredabogacia.htm	digital certificates for lawyers, digital certificates for administrative employees, digital certificates for corporate persons or entities
	Banesto		http://ca.banesto.es/	digital certificates for corporate persons or entities, digital certificates for natural persons or clients
	SCR (Servicio de Certificación de los Registradores)		http://www.scregistradores.com/index.html	n.a.

[750] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

There are also some private Certification Services Providers that are operating in Spain (table 91).

Table 91: Private Certification Service Provider in Spain, source: own illustration

Certification Service Provider		Web page	Issued Certificates
AC CAMERFIRMA		http://www.camerfirma.com/certificatesfeder/	digital certificates to cooperate persons or entities
Firma Profesional		http://www.firmaprofesional.com	digital certificates with einrolement in professional bodies
ANCERT - Agencia Notarial de Certificación		http://www.ancert.com	digital certificate for notary personal and corporate persons and entities, digital certificates for public corporations, digital certificates for employees
ACA - Autoridad de certificación del Consejo General de la Abogacia		http://www.acabogacia.org/acaPublico/publica/index.htm	digital certificates for lawyers, digital certificates for administrative employees, digital certificates for corporate persons or entities
ANF AC		http://www.anf.es/security/cont.html?lang=es	digital certificates for natural persons, digital certificates for corporate persons or entities
Banesto		http://ca.banesto.es	digital certificates for Corporate persons or entities, digital certificates for natural persons for clients

Also the Agencia Tributaria is issuing certificates in Spain (table 92).

Table 92: Certification Service Provider in Spain, source: own illustration

Certification Service Provider		Web page	Issued Certificates
Agencia Tributaria		http://www.aeat.es	n.a.

Inspecting authorities

Agencia Tributaria (AEAT) authorizes the certification service providers.

2.25.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

In Spain, eID cards (figure 87) are issued, but still few people use them.[751]

In March 2006, the eID card was implemented at Burgos. Currently it is only operative in parts of northern Spain.
Until November 2006, around 90.000 eID cards have been issued within 30 offices of 24 cities.
Since September 2006, citizens can use over 260 electronic services that require electronic signature. All services that can be accessed with an eID card are listed at http://www.dnielectronico.es/servicios_disponibles/.[752]

To be able to use the card, a card reader is required as well as a middleware, available for Windows, Linux and MacOS X.[753]

Figure 87: Spanish eID card, source: http://www.dnielectronico.es/, access on 11.12.2007, 09:23

The Oficina Técnia del DNI electrónico coordinates the use of the Spanish eID cards.[754]

The eID card fulfills two different functions: Authentication and signature. Therefore it stores three electronic certificates: the component certificate, the authenticate certificate and the signature certificate, already described in chapter Spain - Application requirements - Types of certificates.

All eGovernment applications at State level that use the eID card are listed in Appendix - Spain: eGovernment using the eID card at State level. Specific applications that are ready for using eID cards can bee seen at http://www.dnielectronico.es/servicios_disponibles/serv_disp_age.html.[755]

Card readers

n.a.

---

[751] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

[752] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[753] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

[754] for more information see http://www.dnielectronico.es/

[755] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Certificate requirements

To use the ID card, a middleware is required, available for Windows, Linux and MacOS X. When connecting to the service through a web browser, the web application is downloaded. With suitable certificate, the user can fill out a web form containing his declaration or import a file generated by other application. When finalized the browser request authorization to use the private key to create a signature, at which point the web form will be signed and sent to the tax authorities.

Many declarations are sending to the server of the AEAT via internet. The signing is done using crypto.signtext with Javascript in Mozilla, Netscape, Firefox and compatibles. In Internet Explorer is done using methods of CryptoAPI that are called trough an ActiveX control.[756]

Application programming interface for online-verification

The Agencia Tributaria offers certification revocation lists.[757]

The issue of the eID card was complemented by creating a multiPKI Validation Platform that provides a free validation service to currently 180 eGovernment services.
The Ministry of Public Administration provides a multiPKI Validation Platform that validates electronic Signatures and electronic certificates to eGovernment services issued by certification Authorities. The platform validates eSignatures and eCertificates issued by the Certification Services Providers. It also offers time-stamping services and a program that enables citizens to sign documents electronically.[758]

The Registro Telematico system requires advanced electronic signatures that are issued by the FNMT Royal Mint. FNMT validates the certificates, the Ministry verifies the signature. Th type of validation protocols is LDAP.[759]

2.25.4 Summary

Table 93 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 93: Summary and rating, Spain, source: own illustration

categories		rating
legal framework	The basis for electronic signatures was created by the Law for electronic signatures in 2003.	A

[756] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

[757] cf. Correspondence with Mr. Luis, Agencia Tributaria, Departamento de Informática Tributaria, Spain

[758] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[759] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Spain, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

categories		rating
technical standard	eGovernment, MultiPKI platform, 180 eGovernment services all autonomous communities have own Internet portals, some of them using electronic signatures. 260 electronic services that require electronic signature, eTax, a lot of other eServices qualified certificates (SW, HW) 15 accredited CSP, 56 types of electronic certificates eID card, smartcards, CRL, OCSP, LDAP	A
distribution	eGov: 17 autonomous communities have own Internet Portal, 12 provide eGov services using eSiganture, 4 adapted the use of eID cards. More than 98% of the taxpayers use the eTax system of the Agencia Tributaria that helps taxpayers to calculates all data In 2005, about 1.375.126 annual VAT income Tax declarations and 1.989.693 periodical VAT income tax declarations have been accepted electronically, using smardcards or software certificates. Until November 2006, around 90.000 eID cards have been issued within 30 offices of 24 cities. The eID card s used very rarely, most people use software certificates. Avanz@ system: per year, 1.500 users with eS use the system. Until now, the CSP FNMT Ceres has issued 1.654.556 certificates.	A

2.26 Sweden

Figure 88: Fact-sheet: Sweden, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:54

In figure 88 some basic demographic and geographic data of the country is presented.

2.26.1 Institutional frame

Legislation

The EU-directive on Electronic Signature was implemented January 1 2001 (see Appendix – Sweden: Qualified Electronic Signature Act).

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Sweden: National Regulations Details.[760]

[760] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•recognition of foreign certificates:[761]
In March 1998, the agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:
Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of Online Services

•eGovernment:
eGovernment services are high in the agenda of Swedish government and. Progress could been made in developing e-services. Verva was selected by the Swedish government to stimulate the use of these services and recently launched a project „The e-society and the organizations“ to enable organizations at municipality level the use of e-services.[762]

➡Short description: Verva[763]
Verva, established in January 2006, is responsible for coordinating the development of central government in Sweden and is one of the Government's central advisory agencies. As the expert in the field of public administration development, the agency intervenes in several key areas, including: eGovernment; strategies to connect citizens and authorities; public procurement coordination in the area of information and communication technology (ICT).

•SAMSET
The Natioal Tax Board was one of the first authorities to offer e-services. In 2002, it was commissioned to coordinate and administrate the certificates for e-signature and e-identification within the government administration. The assignment was effected in collaboration known under SAMSET, including the National Tax Board, the Social Insurance Agency, the Patent and Registries Office and the Swedish Agency for Public Management. Reports concerning the project SAMSET can be found at the website of

[761] cf. Study of the Donau Universität Krems, Master-Studie, Austria

[762] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[763] cf. eGovernment Factsheet (2006)

the National Tax Board http://www.skatteverket.se/.[764]
The National Tax board was one of the first to provide e-services in large scale. One example is the application for personal income tax declaration. Taxes can be declared on the website of the Tax Board (http://www.skatteverket.se) with using either personal security code or eID. In 2006, about 2,7 million tax declarations have been submitted electronically (including about 440.000 using eID).[765]

•Företagsregistrering:[766]
To give a better service to businesses, the Company Registration eService was implemented in cooperation between the Companies Registration Office (Bolagsverket) and the National Tax Board (Skatteverket. The platform is a single point for applications filling and to create application that are signed with electronic signatures. Advanced signatures are required but also qualified certificates are supported. About 20 % of all data on establishment of new companies are filled in electronically per week.

All operational and planned eGovernment applications are listed up in the Appendix - Sweden: Operational and planned applications.[767]

The main application for electronic signature is eGovernment. Several institutions in the public sector use electronic signature, like

- Swedish tax administration (ex. VAT, income tax return, tax account, population register)
- Swedish social insurance administration (ex. child allowance)
- national authority to handle Swedish financial aid for students (ex. loans, grants for studies, recruitment)
- Swedish company registration office (ex. Starting a company including a join up service with the tax administration)
- Swedish Energy Agency (dealing with environment friendly energy)
- Swedish Financial Supervisory Authority (financial institutes reporting to the authority)
- Swedish road administration (car registry)
- Country Council in Stockholm regarding professional chauffeurs (joined up service)
- Guide to Health Care („Vardguiden“, a common portal for the healthcare sector in Stockholm)
- a number of municipalities (services in different areas, like applying for school or nursery) like Nacka, Vaggeryd, Umea etc.

Also some institutions in the private sector is using electronic signature for

---

[764] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[765] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[766] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[767] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

- banking services
- other financial services
- SBAB, applying for residential mortgage
- Adressändring (official change your address company)
- Minpension.se, a public private partnership between government and insurance companies about pensions.

An updated list of all applications (in Swedish) can be found on the website http://www.e-legitimation.se.[768]

Types of electronic signature

The most common ones are advanced electronic signatures, which aren't based on qualified certificates.[769]

The Company Registration eService system requires advanced electronic signature but also qualified signatures are supported. The signatures are only eID based on software solutions.[770]

The Income tax declaration system probably has the most number of users. This year, some 3.584.052 persons used electronic means. If changes are made in pre-filled forms, the use of advanced electronic signature is required and 788.00 people used electronic signatures.[771]

2.26.2 Application requirements

Types of certificates

There are advanced certificates. There is a mixture of soft stored and smart card stored certificates e.g., private keys. The usage of the certificate requires PIN-code and a client side software (installed on the client side, earlier also available as a java applet from some CSPs). Each individual has two key pairs and two certificates (one key pair/certificate for authentication and one key pair/certificate for advanced electronic signature).[772]

By October 2006, about 1.2 million certificates have been issued for e-services, 130000 of them on ID cards.[773]

The names of eIDs are different, depending on the issuer. like BankID or the Steria eID.

---

[768] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

[769] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

[770] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[771] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

[772] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

[773] cf. http://www.vaestorekisterikeskus.fi/vrk/fineid/files.nsf/files/AB5241964425FBF1C2257 2ED001B9EDC/$file/4_Summary+of+the+country+updates.pdf, access on 21.08.2007, 23:24

- Nordea eID:
  The certificate meets the X509v3 standard. The user of eID uses two certificates, one for authentication, another for signing.
  The Certification Policy and Certification Practice Statement can be found at http://www.nordea.se/sitemod/upload/root/se_org/e-legitimation/resurs/medcert.pdf.
- Steria eID:
  The certificate meets the X509v3 standard. The user of eID uses two certificates, one for authentication, another for signing.
  The Certification Policy and Certification Practice Statement can be found at http://eid.steria.se/index.php?page=legal&sessionID=30de23b7b1385ca9f464fca2503fd70d.
- BankID eID:
  The certificate meets the X509v3 standard. The user of eID uses two certificates, one for authentication, another for signing.
- TeliaSonera eID:
  The certificate meets the X509v3 standard.[774]

Around one million swedes use the eID to make about 2,5 million transactions per month for egovernment and other eServices.[775]

But actually, there are no qualified certificates available on the Swedish market. All prerequisites are available but there has been no market openings.[776]
Around 100.000 non-qualified certificates have been issued by Sweden Post, Telia and banks for eGovernment applications and eTax declarations.[777]
During 2006, certificates have been used for approximately 2.5 million transactions per month, for authentication and identification or transactions for advanced electronic signatures. Roughly 1/5 of the total amount of transactions are used for advanced electronic signatures.
Currently about 2,5 million valid certificates for advanced electronic signatures have been issued. There is a mix of hardware and software stored private keys, probably less than 20% are hardware stored. These certificates have been issued to citizens but can also be used for business purposes.[778]

The agency that responsible for the demands on software certificates is Verva - The Swedish Administrative Development Agency (http://www.verva.se).[779]

---

[774] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[775] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[776] cf. Correspondence with Göran Ribbegard, Strategic Analysis Officer, Verva, Swedish Administrative Development Agency

[777] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[778] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

[779] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

Certification Service Providers

There are approximately 10 CSPs in Sweden but none of them are formally accredited. But most of them are recognized by government bodies as a part of public procurement (framework agreement) of identity and signature services.[780]

None of these Certification Service Providers are issuing qualified certificates.[781] Therefore, some activities have been started.[782]

Certificates for eID are issued by Swedish banks (BankID and Nordea), TeliaSonera and Steria.[783]

Table 94 lists up all certification service providers in Sweden.

Table 94: Certification Service Provider in Sweden, source: own illustration

Certification Service Provider		Issued Certificates
BankID	Finansiell ID-Teknik BID AB	eID
Nordea Bank	Nordea	eID
Telia Sonera Sweden	TeliaSonera	eID
Steria	steria	eID

Inspecting authorities

The Body responsible for voluntary accreditation is the Swedish Board for Accreditation and Conformity Assessment (SWEDAC).

The Body responsible for supervision is Post- och telestyrelsen, the National Post and Telecom Agency.

➡Short description: National Post and Telecom Agency

The National Post and Telecom Agency (PTS) is the Swedish supervisory authority for CSPs issuing qualified certificates. There is currently no CA/CSP issuing qualified certificates in Sweden.[784]

2.26.3 Technical preconditions

Signature Software

n.a.

---

[780] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

[781] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

[782] cf. Correspondence with Gunnar Lindstrom, Swedac, Sweden

[783] cf. http://www.vaestorekisterikeskus.fi/vrk/fineid/files.nsf/files/AB5241964425FBF1C22572E D001B9EDC/$file/4_Summary+of+the+country+updates.pdf, access on 21.08.2007, 23:24

[784] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

Types of secure signature-creation device

The National Post and Telecom Agency does not currently recommend, require or support any secure signature-creation device.

•Swedish eID card:

In October 2005, the Swedish government implemented an electronic ID card that contains biometrics data. This card does not replace previous ID cards on paper. The new ID card is used to proof the identity and citizenship. It is also valid as travel document within the Schengen area. The card contains a chip, that my be used to access eGovernment services. [785]

By October 2006, two million cards with electronic identity have been issued.[786]

The eIDs are named after the issuer, like the BAnkID eID, Nordea eID etc.

- Nordea eID:
  Nordea eIDs can be stored on smartcards or saved as files on the hard disc. Nordea uses the card Setec TAG AB and the operating system SetCOS v. 4.4.1 or the Nordea BAnk Card (XponCard) in line with the operation system Proton Prisma EMV.
- Steria eID:
  The eIDs are named after the issuer, like the BAnkID eID, Nordea eID etc.
  Steria eIDs can be stored on smartcards or saved as files on the hard disc The cards use the operating system SetCOS or Cryptoflex from Axalto.
- BankID eID:
  The eIDs are named after the issuer, like the BAnkID eID, Nordea eID etc.
  BankID eIDs can be stored on smartcards or saved as files on the hard disc. Te smart cards are provided y Setec and use the operation system SetCOS v4.4.1 32K.
- TeliaSonera eID:
  The eIDs are named after the issuer, like the BAnkID eID, Nordea eID etc.
  Nordea eIDs can be stored on smartcards or saved as files on the hard disc. Nordea uses the card Setec TAG AB and the operating system SetCOS v. 4.4.1 or SetCOS version 4.3.1.[787]

Card readers

The certification service providers issue eID certificates and recommend the following smart card readers:[788]

---

[785] cf. eGovernment Factsheet (2006)

[786] cf. http://www.vaestorekisterikeskus.fi/vrk/fineid/files.nsf/files/AB5241964425FBF1C2 2572ED001B9EDC/$file/4_Summary+of+the+country+updates.pdf, access on 21.08.2007, 23:24

[787] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[788] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

- Nordea eID:
  For the smartcards used by Nordea for eID, all PC/SC card readers can be used, but Nordea supports Todos Argos Mini II.
- Steria eID:
  For smartcards for the Steria eID, all PC/SC card readers can be used.
- BankID:
  For the smartcards, every PS/SC card reader can be used.
- TeliaSonera eID:
  For the smartcards all PC/SC card readers can be used, but TeliaSonera provides the following card readers:GemPC SB-SL, GemPC Seriel-SL and GemPC Card.

Certificate requirements

•middleware:

The different eIDs are named after the issuing Certification Authority. The certificates are stored on smartcards or directly on the hard disk. To access the certificates a special middleware is required for some of the eIDs:

- Nordea eID: For Nordea eID Nordea uses the middleware Nexus Personal.
- Steria eID: Steria provides PKI client middleware.
- BankID eID: BankID provides a plug-in for authentication and signature that must be used.[789]

Application programming interface for online-verification

There is a standardized API for on-line verification and check of revocation regardless of the CSP uses CRL or OCSP.

Most CAs in Sweden uses OCSP but some of them use CRL.[790]

- Nordea eID:
  For validation of the signature, an online certificate status proocol or a certificate revocation list can be used.
- Steria eID:
  For validation of the signature, certificate revocation list can be used, an Online certificate status protocol services is planned in the future.
- BankID eID:
  For validation of BankID eID, an Online Certificate Status Protocol is used.
- TeliaSonera eID:
  For validation of TeliaSonera eID, an Online Certificate Status Protocol can be used. For older signatures, a certification revocation list is still used.

[789] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[790] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

To simplify adjustments between the IT environment of the eID card supplier and the offered e-services, a specific verification software has been developed. With this software e-services can handled easier in regard of authentication and e-signature. The idea was the development of a general software for all available eID systems. [791]

The most spread solution in Sweden requires a software that is provided by the CSP. Currently most spread is Nexus Personal.[792]

Another possibility is the access of verification functionality via Infra Service provided by TietoEnator and WM-data. The aim is that customers only need to contact the service supplier that verifies the eID for all different eID suppliers.[793]

2.26.4 Summary

Table 95 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 95: Summary and rating, Sweden, source: own illustration

categories		rating
legal framework	The EU-directive on Electronic Signature was implemented in 2001.	A
technical standard	eGov projects, eTax first eService Advanced electronic signature, not based on qualified certificates no qualified certificates available on Swedish market hardware and software certificates 10 (!) CAs 2005, implementation of eID card, also contains biometric data CRL, OCSP	B
distribution	several institutions in public sector use eS, also some in private sector common signature: advanced eS not based on qualified certificates eTax: first eService, in 2006, about 2,7 million tax declarations have been submitted electronically (440.000 using eID) By October 2006, about 1.2 million certificates have been issued for e-services, 130.000 on ID cards. Around 100.000 non-qualified certificates have been issued. Around 1 million Swedes use eID to make 2,5 million transactions per month for eGov and eServices. 1/5 of these transactions are used for advanced eS. Currently, about 2,5 mio certificates for advanced eS have been issued (20% HW stored). By October 2006, 2 million eID cards have been issued.	A

[791] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[792] cf. Correspondence with Björn Scharin, National Post and Telecom Agency Network Security Department, Sweden

[793] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Sweden, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

2.27 United Kingdom

Figure 89: Fact-sheet: United Kingdom, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:54

In figure 89 some basic demographic and geographic data of the country is presented.

2.27.1 Institutional frame

Legislation

The EU-directive was implemented in the Electronic Signatures Regulations 2002, which went into force on the 8. March 2002. (see Appendix – The United Kingdom: Electronic Signature Regulation). Furthermore, the Signature directive was implemented through the „Electronic Communications Act 2000“ (see Appendix – The United Kingdom: Electronic Communications Act).

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - United Kingdom: National Regulations Details.[794]

[794] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

•recognition of foreign certificates:[795]
In March 1998, the agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:
Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of online services

•eGovernment:[796]
The UK Government supports an eGovernment portal approach. The new portal is named „Government Gateway“ on that users can register for eGovernment services. On 25 January 2001, the gateway was launched with the help of a range of partners like Micorosoft, Dell, Cable and Wireless and SchlumbergerSEMA and the eEcnvoy‘s eDelivery team.
The Government Gateway enables registered uses to submit forms electronically to government departments, like the Employers and Electronic VAT Returns.
The user can log on either via User ID and Password or use a digital certificate.
The signature used is only simple and relies on software certificates. Therefore no hardware requirements are assumed. The Certificates must comply with the X.509 Standards.
The design of the portal can be seen in figure 90.
Between February 2001 and June 2005, over 6.8 million active registrations have been effected. From 2003 to 2005, more than 12.1 millions authentications and 152.000 transactions over 5.9 million pounds have been realized. About the use of electronic signatures no statistics could be found.

[795] cf. Study of the Donau Universität Krems, Master-Studie, Austria

[796] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile UK, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

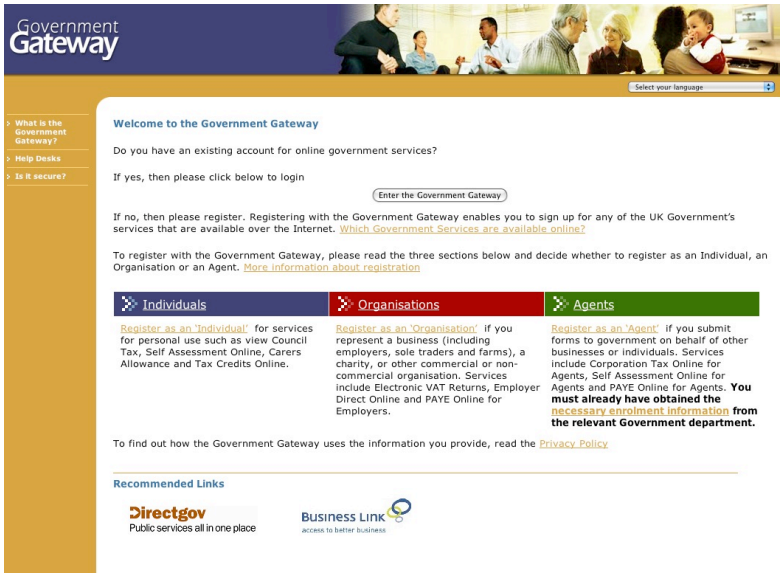


Figure 90: Government Gateway, source: http://www.gateway.gov.uk/, access on 18.12.2007, 13:34

•eVoting:[797]

In 2002, 15 electronic test voting have been carried out in different modes, in 2003, these have been enlarged importantly: Over 160.000 voters have participated. Thereby, online test voting represented the greatest part of votes. Also here, different modes have been used and the access codes have ben sent via postal service.

•e-Conveyancing:[798]

Over a number of years, ideas for reengineering the conveyancing system have been developing to easier conveyancing for all. The aim was to develop a system where citizen, conveyancing professionals and others can easily buy and sell houses. A prototype was developed with a document authentication element that requires electronic signature. The first signature was created in August 2005.

The project was formally closed in November 2005 and is currently phased implemented. More information can be found on the Land Registry website and a evaluation report can be downloaded at http://www.landregistry.gov.uk/assets/library/documents/evaluation_report_version_1.2_sb.pdf.

•other eServices:

All operational and planned eGovernment applications are summed up in the Appendix - United Kingdom: Operational and planned applications.[799]

[797] cf. Arbeitsgruppe E-Voting im BMI, Unterarbeitsgruppe Internationales, Bericht (T.M. Buchsbaum), 20.10.2004

[798] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile United Kingdome, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[799] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Types of electronic signature

SEIS (secured electronic information in society) describes the technical standards and requirements for digital signature.

Both eGovernment Gateway and the eConveyancing system only use simple electronic signature.[800]

2.27.2 Application requirements

Types of certificates

Secure Mark, partner of Geotrust, offers eBusinessID Webserver Certificates, based on SSL certificates.[801]

The certificates that are required for the Government Gateway are software certificates[802]

Certification Service Providers

On the webpage http://www.adreu.eurid.eu/html/en/adr/electronic_signatures/PDF1.pdf you can find a list of certification service providers:[803]

- Trust Assured - The Royal Bank of Scotland plc.
  Certificate Factory - Trustis Limited
  OnSite (Managed PKI) Service
  SecureMark

Table 96 lists up all certification service providers in the United Kingdom.

Table 96: Certification Service Provider in The United Kingdom, source: own illustration

Certification Service Provider		Issued Certificates
Trust Assured	TrustAssured	n.a.
Certificate Factory	trustis	SSL Certificates Personal Certificates
OnSite (Managed PKI) Services	BT	n.a.
SecureMark	SecureMark	n.a.

[800] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile United Kingdome, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[801] cf. http://www.equifaxsecure.co.uk/digitalcertificates/dc_webservcert.html, access on 27.06.07, 14:14

[802] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile UK, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[803] cf. Correspondence with Gerhard K. Müller,, commercial attaché for the United Kingdom, Federal Economic Chamber, foreign trade office, London

Inspecting authorities

The body for voluntary accreditation is the tScheme Limited.

The body responsible for supervision is the department of Trade and Industry.

2.27.3 Technical preconditions

Signature Software

FormPipe is a software based Internet solution for transmitting, receiving and digitally signing documents. A security function enables to digitally sign and encrypt any document.

Types of secure signature-creation device

•E-ID card:

Until November 2006, no electronic ID cards have been issued. implementation of the cards is planned from 2008–2009.[804]

Card readers

n.a.

Certificate requirements

The software certificates that are used for authentication at the Government Gateway require no hardware like smartcards or tokens. Software requirements are:

- Windows 95 or NT 4 (SP3) or higher,
- Internet Explorer 5.01 or above.[805]

Application programming interface for online-verification

Trustassured provides an revocation service.[806]

Also Secure Mark offers an CRL on its homepage to check the status of revoke a certificate[807]

---

[804] cf. www.vaestorekisterikeskus.fi/.../4036B970E0CAA61BC2257219004E5639/ $file/Summary_of_the_country_updates.doc, access on 21.08.2007, 23:29

[805] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile UK, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[806] cf. http://www.trustassured.co.uk, 27.06.07, 14:02

[807] cf. http://www.equifaxsecure.co.uk/policies/crlcheck.html, access on 27.07.07, 14:12

2.27.4 Summary

Table 97 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 97: Summary and rating, United Kingdom, source: own illustration

categories		rating
legal framework	The EU-directive on Electronic Signatures was implemented in 2002.	A
technical standard	eGov gateway, login only via ID/password of digital software certificate (simple electronic signature), eVoting, eConveyancing simple signature based on software certificates, smart card or USB token implementation of eID card for eServices planned 2008/2009 4 certification service providers CRL	C
distribution	Between February 2001 and June 2005, over 6.8 million active registrations have been effected. From 2003 to 2005, more than 12.1 millions authentications and 152.000 transactions over 5.9 million pounds have been realised no statistics on use of electronic signatures	-

3 Country Analysis: EU member candidates

3.1 Croatia

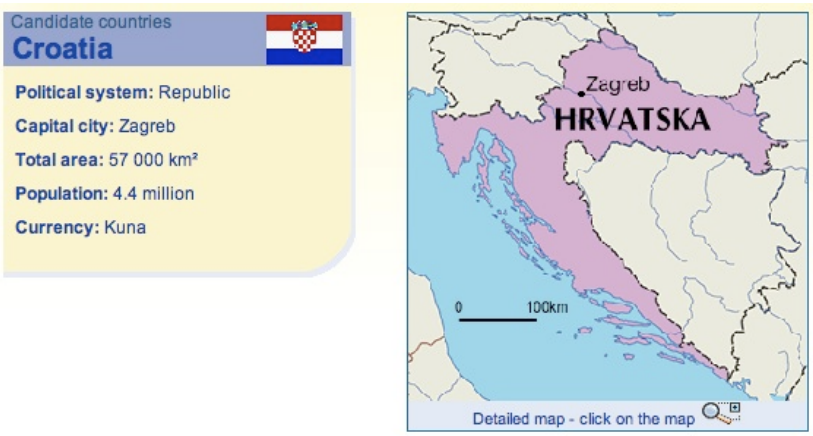


Figure 91: Fact-sheet: Croatia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:54

In figure 91 some basic demographic and geographic data of the country is presented.

3.1.1 Institutional frame

Legislation

In Croatian national law, EU signature directive was implemented in January, 2002 (Electronic signature act, Narodne novine, no. 10/2002, see Appendix - Croatia: Electronic Signature Act[808]) as part of the harmonization with EU legal requirements. The aim is to support eAdministration and eGovernment.[809]

[808] cf. http://www.e-croatia.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/00/document/eSignature_Act.pdf , access on 19.12.2007, 14:30

[809] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

The Act is accompanied by some regulations for the technical details of valid digital signature:[810]

- „Regulation for registering of persons that offer services for certification of electronic signatures", Narodne novine, no. 54/02
- „Regulation for registering of persons that offer services for certification of electronic signatures that issue qualified certificates", Narodne novine, no. 54/02
- „Regulation of measures and procedures of use and protection of electronic signature and advanced electronic signature, means for creation of electronic signatures, advanced electronic signatures and the system of certification and obligatory insurance of persons that issue qualified certificates", Narodne novine, no. 54/02.

Availability of Online Services

•Internet access:[811]

Since 2002, Croatia is keen on implementing eGovernment and initialized some strategies to make advantages of information technology more visible. To have an effect of information technology, it is necessary that citizens are more involved and to support eCommerce.

A recent study showed that only few people have intern access, namely 18% of the population aged between 10 years and 74 years. But the number is rising, in 2000, only 6.83% had accesses to Internet.

•eGovernment:

The implementation of eGovernment is one of Croatia's priorities.

The implementation requires a legal framework, technical equipment and educated staff.

In 2003, the Central Government Office was established. This body was created to develop a stronger coordination in the use and implementation f computer systems between governmental departments.

But the eGovernment development progress is relatively slow due to insufficient coordination, especially in the area of eCommunication.[812]

One main target is the completion of the government service HITRO.HR for a quick communication between citizens, businesses and state administration.[813]

In May 2007, the Government of Croatia adopted an operation plan for the implementation of the e-Croatia program for 2007. The target is to provide citizens and businesses with the highest level of services, like information, exchange of information and active participation in global developments[814].

---

[810] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[811] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[812] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[813] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[814] cf. http://www.e-hrvatska.hr/sdu/en/ProgramEHrvatska/OPrograma.html, access on 01. 08.2007, 19:21

The majority of state information is now available online, but just information is provided and no real services are accessible.[815]

•eTax:[816]
Croatia recently adopted an electronic VAT declaration system, accessible at http://www.porezna-uprava.hr/e-porezna/ePDV.asp. The system is based on advanced electronic signatures that are issued by FINA. The system requires a client and a special software that signs all messages that are sent to the tax authority and submits the declarations.
But the system is rarely used by private persons, companies are not interested in investing in this system.

•Social security:[817]
The Pension fund offers its clients an electronic declaration service of pension contribution.[818] The system is based on advanced signature certificates of identification. Customers can download empty forms, fill them with necessary data and sign these pdf documents using advanced electronic signature.
The services are used by only few people.

Types of electronic signature

In Croatia, electronic signature is defined almost equally as EU define electronic signature. According to that, basics of electronic signature would be:

Electronic signature signify data series in electronic form which are associated to or logically related with other data in electronic form and are used for signatory identification and authenticity of a signed document. Advanced electronic signature signify electronic signature which fiducially guaranty signatory identity and it is:

- uniquely linked to the signatory
- capable of identifying the signatory
- created using means that the signatory can maintain under his control
- linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.[819]

Common electronic signatures in Croatia are PKI based electronic signatures.

Therefore, customers can use electronic signature for strong authentication and document/data integrity protection, and also according to Law of Electronic Signature, can use advanced electronic signature.

---

[815] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[816] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[817] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[818] see http://www.mirovinsko.hr

[819] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

Advanced electronic signature provides non-repudiation and it is legally equalized with handwriting signature or stamp mark.[820]

For example the electronic tax declaration system as well as the social security system for the declaration of pension contribution and require the use of advanced electronic signatures.[821]

Croatia is mostly using PKI solutions. The legal framework for electronic signature is based on public key technology. But it has no commercial use, and it is not spread widely among the population.[822]

One reason for the limited use of electronic signatures is the lack of technical equipment, detaining governmental departments to use electronic documents or offer digital services.[823]

3.1.2 Application requirements

Types of certificates

The Financial Agency (FINA) enables customers to use secure electronic signature through digital certificates that they provide.

Depending on purpose, it is issuing two types of certificates:
a) Personal certificates – issued for citizens
b) Business certificates – issued for persons, applications, web servers or devices within a corporation or a company.

Depending on usage, it is issuing these types of certificates:
a) Normalized certificates – we gave them a name Authentication/Encryption certificate They are denoted as NC and have Key Usage indication: Key Encipherment, Digital Signature
b) Qualified certificates – we gave them a name Signing certificate They are denoted as Qualified Certificates and have Key Usage indication: Non-Repudiation
c) Secure certificates which are also known as a SSL certificates and they exist for hardware and software certification, as I mentioned before. They are always normalized certificates, because, according to are Law, qualified certificates can be issued only to a person not to a device or application. Also, we can provide secure certificates with different level of security. Therefore, level of certificate security could be standard, medium or high, depending of customer need.

---

[820] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

[821] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[822] cf. http://ec.europa.eu/idabc/servlets/Doc?id=29084, access on 01.08.2007, 19:43

[823] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

FINA's certificates allow safe electronic access to information and services through the application of the public key infrastructure and the technology of electronic signatures.[824]

The e-Vat declaration system requires a qualified certificate.[825]

Certification Service Providers

Certificate Authorities must be registered by the Ministry of Economy and are published on their website http://mingorp.fina.hr. The registration is just a control, the activity of the authority is not limited.[826]

There is one accredited Certification Service Provider that issues qualified certificates: The Financial Agency – FINA.[827]

➡Short description: The Financial Agency (FINA)
It is the leading Croatian company in the sphere of financial mediation. The national coverage, the information technology systems tested in the most demanding operations of national importance and high professional level of expert teams are the major advantages of FINA. These characteristics enable FINA to prepare and implement various projects: from simple financial transactions up to the most sophisticated activities in electronic business operations. The Financial Agency is owned by the State, but it operates exclusively on the market principle. FINA's Digital Certificate Registry is the leading Croatian provider of the service of certification to citizens and business entities. It operates in accordance with the Law on Electronic Signature and is the only authorized certifying institution registered with the Ministry of Economy as the umbrella certifying authority for the Republic of Croatia.[828]

Table 98 lists up all certification service providers in Croatia.

Table 98: Certification Service Provider in Croatia, source: own illustration

Certification Service Provider		Issued Certificates
Financial Agency FINA		Personal certificates Business certificates Normalized certificates Qualified certificates Secure certificates

[824] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

[825] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[826] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[827] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[828] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

The reason for the existence of only one certification authority lies partly in the limited use of advanced electronic signature.[829]

Inspecting authorities

The Government authority, Ministry of Finance, observe the certification service provider.[830]

3.1.3 Technical preconditions

Signature Software

For creating advance electronic signature, in line with regulations, signature software is required. FINA also provides these software, but on the market, customers can find various software application, which are used for signing or/and encrypting documents. Some of them are basic, some of them are advanced.[831]

Types of secure signature-creation device

Social Security developed a service to electronically declare pension contribution. This system requires advanced qualified signature that is issued by FINA and available on Smart cards that are secured by PIN. [832]

FINA is supporting smart card with chip that is required for storage of customer private key. Regarding creation of advance electronic signature, length of key for creating advance electronic signature has to be at least 1024 bit, with cryptography algorithm appliance from class RSA/DSA and coherent with international standard PKCS#1.

Among the others, FINA is also implementing international norm of secure signature creation device, CEN/ISSS SSCD-PP, general norm for protection of device that are creating advance electronic signature, which EU was accepted according to Directive 1999/93, in Annex II.[833]

Twenty seven banks plan to replace magnetic stripe cards with smartcards for e-purse, credit and debit applications.

---

[829] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[830] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

[831] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

[832] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[833] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

•eID:[834]
Electronic identity Cards are not available yet and not in project soon. Afore, all registers and informations must be completely digitalized, which has not been realized yet.

Card readers

FINA is providing GemPC TWIN smart card reader with USB port, although they can ensure serial port if customer needed. However, smart cards are compliant with various card readers so users can choose whether they want to use reader that FINA provides or somebody else. Secure PIN entry is possible for secure electronic signature. Customers are using secure PIN entry via PIN pad on crypto-module where certificate with high-level security is stored.[835]

Certificate requirements

FINA can only recommend that the key length has to be 1024bit. However, FINA does have some specific and necessary demands before issuing a certificate. That would be procedure. Every customer needs to be identified and authenticated before getting a certificate. First step would be registration of a company or organization where legal papers of company existence need to be delivered. During the registration our LRA (Local Registration Authority) perform I&A of company Chairmen. Registration is done on a one-time basis. When company is registered, employees could demand for certificates. For software certificate, each of them has to have so called guardian. He/she needs to complete a form in which specifies demands for certificate. Form has to be signed either by guardian and Chairman. Guardian also is liable to I&A procedure. After passing the required procedure, certificate can be issued.[836]

For creating advance electronic signature, in line with regulations, signature software is required. FINA also provides these software, but on the market, customers can find various software application, which are used for signing or/and encrypting documents. Some of them are basic, some of them are advanced.

The Croatian Government in cooperation with FINA, provides B2G electronic services (e.g., sending VAT forms, Annual report form, registration to pension fond etc.), which has signing software within signing policy already implemented in service. FINA also developed PKI signing modules for advance electronic signature, based on JAVA and PKCS#11 module, which can be implemented directly in other software, applications or systems, such as DMS, ERP etc. So, according to that, other IT companies don't have to develop these types of product of their own to provide entirely solution to their customers. Certificate profiles that are issued in Croatia can be used in standard internet application such as: Microsoft Internet Explorer, Microsoft ´Internet Information Server, Netscape, Netscape WEB server, Mozilla, Appache WEB

[834] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[835] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

[836] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

server (with SSL support). FINA prefers MOS and signature devices can be used in Windows 98SE, Windows ME, Windows 2000 and Windows XP.[837]

The required software needed for the electronic tax declaration system can be downloaded at http://www.porezna-uprava.hr/e-porezna/OvlastenjaFull.asp.[838]

Application programming interface for online-verification

It is recommended to be connected with online CRL list. The list is updating every 6 hours[839]

3.1.4 Summary

Table 99 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 99: Summary and rating, Croatia, source: own illustration

categories		rating
legal framework	The EU-directive on Electronic Signatures was implemented in 2002. national norm of secure signature creation device.	A
technical standard	eGovenrment development is slow due to insufficient coordination, and the lack of technical equipment in governmental departments. eCroatia implementation plan for 2007, until now, only information is available, no real services are accessible, eTax system and Social Security service based on advanced electronic signatures basic and qualified certificates (SW, HW), SSL certificates no eID cards available yet, smartcards 1CSP CRL	B
distribution	Internet access limited ES is not widely used. the eTax system is not used very often as neither private persons nor companies want to invest in this system PKI solutions have no commercial use and are not wide spread among the population.	C

[837] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

[838] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Croatia, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[839] cf. Correspondence with Andreja Kajtaz, Division Adviser, Customer service Division of the Financial Agency in Croatia

3.2 Republic of Macedonia

Figure 92: Fact-sheet: Republic of Macedonia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:55

In figure 92 some basic demographic and geographic data of the country is presented.

3.2.1 Institutional frame

Legislation

The EU-directive on digital signatures is only partly implemented in national Law, the Law on Data in Electronic Form and Electronic Signature and related bylaws in 2001.[840]
The Law on Data in Electronic Form and Electronic Signature can be found in the Appendix - MAcedonia: eSignature Law)[841]

Availability of Online Services

•eGovernment Project:
Macedonia recognizes that an existence of an e-society is very important and undertook several steps in this direction.[842]

The US Agency for International Development (USAID) founded an e-Government Project (figure 93) with the goal to increase the transparency and efficiency of public sector management and making Macedonia more attractive for Investors by open new channels of doing business in a secure manner.[843]

[840] cf. Correspondence with Dr. Josef Treml, commercial attaché, Federal Economic Chamber, foreign trade office Belgrade

[841] cf. http://www.finance.gov.mk/gb/laws/law_on_data_in_electronic_form_and_electronic_signature.pdf, access on 19.12.2007, 15:20

[842] cf. http://www.pwc.com/extweb/industry.nsf/docid/5891e985db830b3c802570c10051f954, access on 01.08.07, 10:24

[843] cf. http://www.e-gov.org.mk/about.htm, access on 01.08.07, 10:19

Legislation concerning electronic data has been in place since 2001, necessary laws have been modified to permit digital signature. Also steps for instituting the first public Certification Authority have been taken.[844]

Figure 93: eGovernment, Macedonia, source: http://www.e-gov.org.mk/about.htm, access on 05.09.2007, 19:26

Some banks are already offering an e-banking service, others are developing such services. [845]

Types of electronic signature

Currently, no adequate system exists in Macedonia, that issues certificates on electronic signatures.[846]

3.2.2 Application requirements

Types of certificates

When using the eGovernment services, digital certificates serve as authentication. The user can log in via a Pin number, the system automatically checks the validity and the user will be identified.[847]

MT, Makedonski Telekomunikacii, is the leading telecom provider in Macedonia. To further the development of electronic services in Macedonia, MT has build a system for developing a PKI and issuing digital certificates. These digital certificates do meet the standards of the Law on Data in Electronic Form and Electronic Signature.

---

[844] cf. http://www.pwc.com/extweb/industry.nsf/docid/5891e985db830b3c802570c10051f954, access on 01.08.07, 10:24

[845] cf. http://www.pwc.com/extweb/industry.nsf/docid/5891e985db830b3c802570c10051f954, access on 01.08.07, 10:24

[846] cf. Correspondence with Dr. Josef Treml, commercial attaché, Federal Economic Chamber, foreign trade office Belgrade

[847] cf. http://www.e-gov.org.mk/tender_q&a_summaray.htm, access on 01.08.07, 10:21

The certificates are qualified and standardized. They are compatible with all systems that use digital certificates, like bank applications or e-commerce applications. [848]

MT offers qualified certificates for mass use and normalized digital certificates for technical use (table 100):

Table 100: Types of certificates issued by MT, source: http://www.mt.com.mk/eng/ca/TipoviNaMTSertifikati.asp?id=679, access on 25.08.2007, 12:11

CSP	Issued C	type	specification
MT	qualified C	MTnet KS	qualified certificate intended for standard applications can be used for: • secure e-mail • encryption/decryption of files • digital signature • e-payment/e-commerce. certificate validity: one year, with the ability to renew for one year (no more than 4 consecutive renewals) insurance – the certificate is insured to an annual amount of € 50,000.
		MTnet KS+	qualified certificate with obligatory use of token that provides increased security for keeping the certificate same characteristics as MTnet KS, only the certificate is kept on a token intended for standard applications can be used for: • secure e-mail • encryption/decryption of files • digital signature • e-payment/e-commerce. certificate validity: one year with the ability to renew for one year (no more than 4 consecutive renewals) insurance – the certificate is insured to an annual amount of € 100,000.
		MTnet KSN	advanced qualified certificate intended for advanced applications can be used for: • secure e-mail • encryption/decryption of files • digital signature • securing numerous types of digital data • VPN authorisation • domain authorisation • e-payment/e-commerce certificate validity: one year, with the ability to renew for one year (no more than 4 consecutive renewals) insurance – the certificate is insured to an annual amount of € 150,000.

[848] cf. http://www.mt.com.mk/eng/ca/digitalnisertifikati.asp?id=661, access on 01.08.07, 10:54

CSP	Issued C	type	specification
		MTnet KSN+	advanced qualified certificate with obligatory use of token that provides increased security for keeping the certificate same characteristics as MTnet KSN, only the certificate is kept on a token intended for advanced applications can be used for: • secure e-mail • encryption/decryption of files • digital signature • securing numerous types of digital data • VPN authorisation • domain authorisation • e-payment/e-commerce certificate validity: one year, with the ability to renew for one year (no more than 4 consecutive renewals) insurance – the certificate is insured to an annual amount of € 200,000.
	Normalized certificates	MTnet SSL NS	normalized certificate for technical use for SSL communication can be used for creating HTTPS communication for hosting web sites with secure content certificate validity: one year with the ability to renew for one year (no more than 4 consecutive renewals) insurance – the certificate is insured to an annual amount of € 200,000
		MTnet VPN NS	normalized certificate for technical use for secure VPN networks can be used to create Virtual Private Networks (VPN) for secure data transfer through public networks certificate validity: one year, with the ability to renew for one year (no more than 4 consecutive renewals) insurance – the certificate is insured to an annual amount of € 200,000.
		MTnet CS NS	normalized certificate for signing software intended for software developers can be used for confirming the software code user identity certificate validity: one year, with the ability to renew for one year (no more than 4 consecutive renewals) insurance – the certificate is insured to an annual amount of € 200,000.

Certification Service Providers

Some private companies began to issue certificates, but they lack the right to do so.[849]
AD Makedonski Telekomunikacii issues digital certificates that meet the standards.

➡Short description: MT, Makedonski Telekomunikacii[850]
It is the leading telecom provider in Macedonia, which integrates its know-how with Information and Communications Technology to provide its customers with hi performance solutions.

[849] cf. Correspondence with Dr. Josef Treml, commercial attaché, Federal Economic Chamber, foreign trade office Belgrade

[850] cf. http://www.mt.com.mk/eng/ca/digitalnisertifikati.asp?id=661, access on 01.08.07, 10:54

Table 101 lists up all certification service providers in Macedonia.

Table 101: Certification Service Provider in the Republic of Macedonia, source: own illustration

Certification Service Provider		Issued Certificates
Makedonski Telekomunikacii		qualified certificates advanced qualified certificates normalized certificates - for SSL communication - for VPN Networks - for signature software

Inspecting authorities

n.a.

3.2.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

MT offers a MTnet KS+ and MTnet KSN+ qualified certificate that can obligatory used with token.[851]

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

3.2.4 Summary

Table 102 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

[851] cf. http://www.mt.com.mk/eng/ca/TipoviNaMTSertifikati.asp?id=679, access on 25.08.07, 12:11

Table 102: Summary and rating, Republic of Macedonia, source: own illustration

categories		rating
legal framework	The EU-directive on Electronic Signatures was only partly implemented in 2001. Some companies began to issue certificates, but without the right to do so. digital signature is permitted	B
technical standard	eGov initiatives were taken, eGov services with only PIN authentication, Currently no adequate system to issue certificates, building up a system for developing PKI and issuing digital certificates, only one CSP that issues digital certificates that meets the standards. issues basic and qualified certificates, SSL certificates, software certificates token	C
distribution	-	-

3.3 Turkey

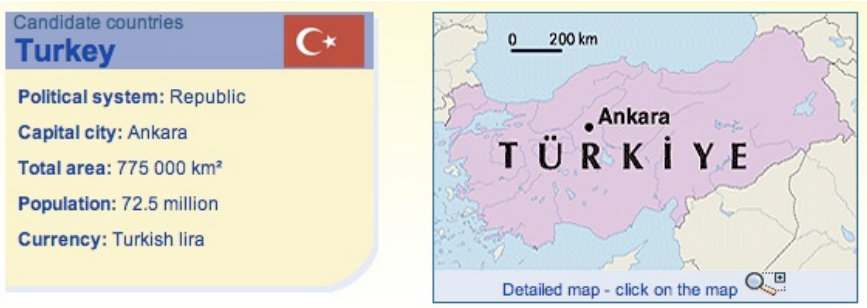


Figure 94: Fact-sheet: Turkey, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:55

In figure 94 some basic demographic and geographic data of the country is presented.

3.3.1 Institutional frame

Legislation

The Turkish Law on electronic Signatures (see Appendix – Turkey: Law on Electronic Signature) was implemented in 2004.

Qualified electronic signatures have the same legal value as handwritten ones.[852]

All national regulations concerning eCommerce, eGovernment and electronic signatures can be found in detail in the Appendix - Turkey: National Regulations Details.[853]

•Recognition of foreign certificates:[854]

To accept foreign certificates, either an international agreement or a surety of a domestic certification service provider is required. The Turkish Act regulates that certificates that are accepted by a domestic certification service provider in Turkey, they are hold as qualified certificates and both CSP - local and foreign - are liable for damages caused by using the foreign certificates.

To accept foreign certificates some minimum requirements must be fulfilled:

- The foreign certificate must have the same technical specifications like a qualified certificate.
- The certificate issuer must be a certification service provider in its own country.

---

[852] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Turkey, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[853] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[854] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Turkey, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

- The Certification Service Provider that accepts the certificate in Turkey must submit all information to the Telecommunication Board one month before accepting it.
- The foreign Certification Service Provider must submit a certificate sample.
- A qualification document of the foreign Certification Service Provider must be provided by the relevant foreign authority as well as
- all documents that prove that the foreign certificates fulfill all technical specifications of a domestic qualified certificate.

The local certification service Provider is jointly liable with the foreign one.

In October 1998, the agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 States have joined the Common Criteria Mutual Recognition Agreement: [855]

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

Availability of Online Services

•eGovernment:

The Turkish Government is keen to ensure that public institutions, organizations and citizens are aware of the benefits of an information society. Thus, eGovernment is one of the main focuses of the government. Projects are underway for many years. Since 2000, many initiatives for building an information society have been effected all around the world and also in Turkey. Turkey is part of the eEurope+ Initiative. The „eTransformation Turkey Project" aims to transform the country into an information society, including all citizens, businesses and public authorities. Therefore, two action plans for 1003-2004 and for 2005 have been launched and implemented successfully. In 2005, another strategy plan covering 2006-2010 has started to define middle and long term strategies along with targets for realization.[856]

•Inward Processing Regime:[857]

After electronic signature was regulated and certification service provider started their operations and secure electronic signature became available, many public organizations started to develop projects to use electronic signature. On of the first project was the Interior Processing Regime Project (IPR Automatonn), initiated by the Undersecretariat of Foreign Trade (UFT). The project was called „eDocuments in Foreign Trade", involving an Inward Processing Permission Certficate. Firms that apply to the UFT fill out those Certificate in form of paper documents. UFT constituted the „Inward Processing

[855] cf. Study of the Donau Universität Krems, Master-Studie, Austria

[856] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Turkey, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[857] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Turkey, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

Regime Project“ to eliminate bureaucratic difficulties and give priority to exportation in government institutions. Information Technologies should be used to increase exportation effectively.
In automation projects of this regime PKI infrastructure is used and therefore the fist project in Turkey making use of electronic signatures and PKI infrastructure. In order to secure the platform for companies, intelligent cards with digital signatures are required (Security Certificate, software certificate, on smartcard or token).

Types of electronic signature

Kamu SM, the governmental CA issues qualified electronic certificates to create secure e-signature.[858]

But there was little awareness of electronic signatures in the business community or Turkish society. In April 2007, government officials announced that only 12,000 electronic-signature certificates had been issued to date.[859]

3.3.2 Application requirements

Types of certificates

•mobile SIM certificates:
Turkcell's m-signature program on Mobile certificates. They enable transactions similar to what a smart card and a card reader accomplishes with a computer. With this mobile certificate, the mobile phone can be used to generate digital signatures.
Secure qualified certificates can be issued based on a digital key pair that is generated on the SIM card of a mobile phone[860].

•Software certificates:[861]
For the only application using electronic signature, software certificates are required, on smart cards or token.

Certification Service Providers

In Turkey there is a governmental Certificate Authority (Kamu Sertifikasyon Merkezi) and three independent certificate authorities that are all issuing qualified digital signature.

---

[858] cf. http://www.kamusm.gov.tr/en, access on 25.07.2007, 23:43

[859] cf. http://globaltechforum.eiu.com/index.asp?layout=rich_story&channelid=4&categoryid=31&title=Turkey%3A+Overview+of+e-commerce&doc_id=11173, access on 01.08.2007, 23:48

[860] cf. http://news.thomasnet.com/companystory/506047,http://www.totaltele.com/iew.aspx?ID=6147&t=1, access on 25.07.2007, 23:25

[861] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Turkey, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

➡Short description: Kamu Sertifikasyon Merkezi[862]
Kamu SM is the governmental certificate authority for all government agents for internal use. It was established in 2005 and was authorized by the Telecommunications Authority. Kamu SM has specialized in qualified certificate services, based on PKI technology.

The other independent CAs are E-Güven, Turktrust and E-Tugra.

➡Short description e-Güven:
e-Güven acts since 2003 as the Turkish qualified Certificate Authority. It was equipped with a certificate management and registration technology that allows to act as a qualified Mobile Certificate Issuer for Turkish citizens.[863]
It is a commercial enterprise that was founded in November 2003 with the aim to establish a security infrastructure in Turkey. It is the firs and the leading CSP in Turkey.

Table 103 lists up all certification service providers in Turkey.

Table 103: Certification Service Provider in Turkey, source: own illustration

Certification Service Provider		Issued Certificates
Kamu SM (Government CA)		Qualified certificates
e-Güven		Qualified certificates qualified mobile certificate
TURKTRUST A.S.		Qualified certificates
EBG Bilisim Teknolojileri ve Hizmetleri A.S.		Qualified certificates

Inspecting authorities

The Body that is responsible for supervision is the Turkish Telecommunication Authority.

3.3.3 Technical preconditions

Signature Software

n.a.

[862] cf.:http://www.kamusm.gov.tr/en, access on 25.07.2007, 23:43

[863] cf. http://news.thomasnet.com/companystory/506047,http://www.totaltele.com/View.aspx?ID=6147&t=1, access on 25.07.2007, 23:25

Types of secure signature-creation device

In Turkey, mobile SIM cards are available with a mobile certificate to create a digital signature.[864]

Card readers

For the „Inward Processing Regime“, software certificates on smartcards or tokens are required. For those, different card readers are recommended: Gemsafe Card Reader, Vasco Card Reader, Omikey Card REader, ACS CArd Reader.[865]

Certificate requirements

n.a.

Application programming interface for online-verification

Kamu SM provides an OCSP server to determine the status of issued certificates, Turktrust a CRL.[866]

3.3.4 Summary

Table 104 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 104: Summary and rating, Turkey, source: own illustration

categories		rating
legal framework	The EU-directive on Electronic Signatures was implemented in 2004.	A
technical standard	eGov in progress, action plans, seceral projects to use eS Qualified certificates for secure electronic signature, eGovernmet in progress, qualified signatures software certificates 1 government CA, 3 independent CSP, issuing qualified certificates smartcard, Token, program on mobile SIM certificates several card readers CRL, OCSP	B
distribution	Little awareness of electronic signatures, only 12.000 electronic signatures have been issued until April 2007.	B

[864] cf. http://news.thomasnet.com/companystory/506047, access on 25.07.2007, 23:25

[865] cf. European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Turkey, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24

[866] cf. http://www.turktrust.com.tr/crl_ain.jsp, access on 25.08.07, 14:25

4 Country Analysis: other European countries

4.1 Albania

Figure 95: Fact-sheet: Albania, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 95 some basic demographic and geographic data of the country is presented.

4.1.1 Institutional frame

Legislation

A law on electronic signature is indispensable for Albania in the digital age. The Prime Minister SalliBerisha adheres that „The law is extremely indispensable for the widespread use of electronic procedures“.[867]

In the area of personal data protection, very little progress has been made. The Law on protection of personal data 1999 is being revised to bring it in line with European standards. However, a supervisory authority for data protection is not n operation yet. The area of protecting personal data is in early stage.

[867] cf. http://gazetastart.com/?faqe=shfaqflash&LajmID=18076, published on 05.01.2008, 16:38, access on 16.01.2008, 11:42

The Act on the Protection of Personal Data can be found in the Appendix - Albania: Law on the Protection of Personal Data.[868]

Availability of Online Services

The area of electronic communication and information technology is not very developed yet.[869]

Types of electronic signature

Electronic Signature is not yet a topic in Albania.[870]

4.1.2 Application requirements

Types of certificates

n.a.

Certification Service Providers

n.a.

Inspecting authorities

n.a.

4.1.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

n.a.

Card readers

n.a.

---

[868] cf. http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.AL, access on 27.06.2007, 12:43

[869] cf. Commission of the European Communities, Albania 2007 Progress Report, 2007

[870] cf. Correspondence with Mag. Christian Miller, commercial attaché for Slovenia and Albania, Federal Economic Chamber, foreign trade office Ljubljana

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

4.1.4 Summary

Table 105 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 105: Summary and rating, Albania, source: own illustration

categories		rating
legal framework	A law on electronic signature is indispensable for Albania in the digital age.	-
technical standard	Electronic Signature is not yet a topic in Albania.	C
distribution	Electronic Signature is not yet a topic in Albania.	C

4.2 Armenia

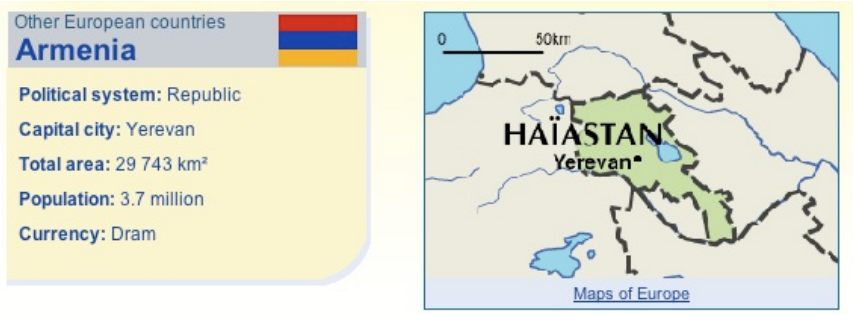


Figure 96: Fact-sheet: Armenia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 96 some basic demographic and geographic data of the country is presented.

4.2.1 Institutional frame

Legislation

The area of Electronic contracts is not uniquely regulated in Armenia. Further there is no specific legislation on e-commerce.[871]

The Republic Armenia Civil Code states that „the use in the concluding a transaction of facsimile reproduction of a signature with the assistance of means of mechanical or other copying, electronic digital signature, or other analogue of an actual handwritten signature is allowed in cases and by the procedure provided by a statue, other legal acts, or agreement of the parties“ (see Republic Armenia Civil Code, downloadable at http://www.parliament.am/legislation.php?sel=show&ID=1556&lang=eng, only an unofficial english translation could be found). That means that the Civil Code authorizes electronic signatures if both parties agree.

The Government has adopted decree that defines that every software manufacturer that is willing to supply encrypting software to governmental agencies has to submit its software to the Ministry of National Security to certify the software. For commercial or non-governmental purposes, no law regulates the production or distribution of the software.[872]

In February 2002, the Armenian Government put a first version of the draft law on electronic signature in circulation, based on the model law that was proposed by the parliamentary assembly. This draft law was

[871] cf. see http://www.gipi.am/?i=243

[872] cf. http://www.american.edu/carmel/hs9920a/armenia/encryption_in_armenia.htm, IT Landscape in Armenia, access on 27.12.2007, 09:02

significantly changed in result of several discussions, organized by a working group of the Ministry of Trade and Economic Development and IT Development Council.[873]

In June 2005, the National Assembly adopted the Law of the Republic of Armenia on Digital Documents and Digital Signatures. The Law takes into account main principles of the EU Directive on Digital Signatures like the voluntary accreditation of CSP and e-signature products.
One problem is the lack of accreditation criteria in the Law and also implementing regulations are adopted only partially: accreditation procedures are defined but accreditation criteria are still being discussed.[874]

All eCommerce indicators (including local legislation) can be found in the Appendix - Armenia: eCommerce indicators.[875]

Availability of Online Services

•Computer Availability:[876]
The cost of equipment and connectivity is a great obstacle for the information society of Armenia. The Armenian Internet Society carried out a survey in 2002 and observed that there are only 1.5 to 2 computers per 100 households in Armenia.

•Internet Access:[877]
In rural areas in armenia, the access to electronic communication services is limited due to the absence of infrastructure as well as service providers. According to a survey in 2004 by the World Bank, only 7 percent of rural communities have access to Internet. In 2005, the survey showed that around 60.00 households have connection to Internet. The Armenian Internet Society suggests that about 5 to 6 percent use the Internet regularly, manly with dial-up connection.

•eCommerce:[878]
The use of xDSL internet connections is limited because of high equipment costs. Most households or businesses use dial-up connections.
Only very few businesses have their own website (for a test sample for this study 3 out of 100 companies) or use online tools for daily operations or communication and sale.

---

[873] cf. Correspondence with Mag. Hans Kausl, commercial attaché for Armenia, Azerbaijan and Georgia and Russia, Federal Economic Chamber, foreign trade office Moscow

[874] cf. Europe‘s Information Society, Political Intelligence Report, Armenia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[875] cf. Correspondence with Mag. Hans Kausl, commercial attaché for Armenia, Azerbaijan and Georgia and Russia, Federal Economic Chamber, foreign trade office Moscow

[876] cf. Europe‘s Information Society, Political Intelligence Report, Armenia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[877] cf. Europe‘s Information Society, Political Intelligence Report, Armenia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[878] cf. Europe‘s Information Society, Political Intelligence Report, Armenia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

In 2001, the Armenian Government declared the IT sector as one priority for the economic development of Armenia, but so far only few measures have been taken to realize progresses.

•eGovernment

EGovernment is at an early development stage in Armenia and not well coordinated.

In June 2001, the government announced ICT to be poor in the country‘s economic development. In 2003, the e-Armenia initiative was launched, but only little progress has been made up to now.[879]

Some e-governance tools have been developed, like the e-visa system, a system to apply for a visa electronically (figure 97, figure 98).[880] It was developed with support of international organizations and was one of the first step of eGovernment. This system enables the issuance of electronic visas, they are submitted and verified online within 2 business days.[881]

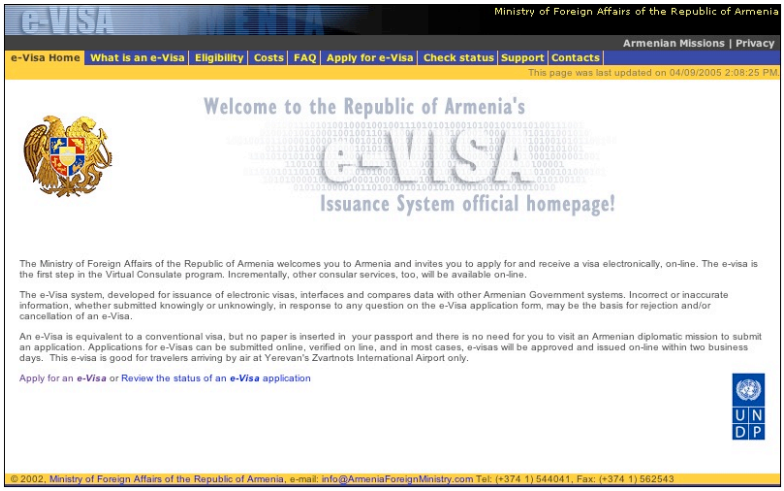


Figure 97: e-Visa, source: http://www.armeniaforeignministry.am/eVisa/, access on 27.12.2007, 09:07

[879] cf. Europe‘s Information Society, Political Intelligence Report, Armenia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[880] cf. Europe‘s Information Society, Political Intelligence Report, Armenia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[881] cf. http://www.armeniaforeignministry.com/eVisa, access on 27.12.2007, 09:02

Figure 98: Apply for e-Visa for Austria, source: https://orderpage.ic3.com/hop/orderform.jsp, access on 27.12.2007, 09:13

Most of the Armenian Ministries and Governmental authorities have their own website, but these are only infrequently updated and mostly only contain general information about the institution. Only few governmental web sites have interactive or communication tools, often limited to email communication systems). Figure 99 shows the eGovernment site of Armenia, that contains governmental decisions and press releases.[882]

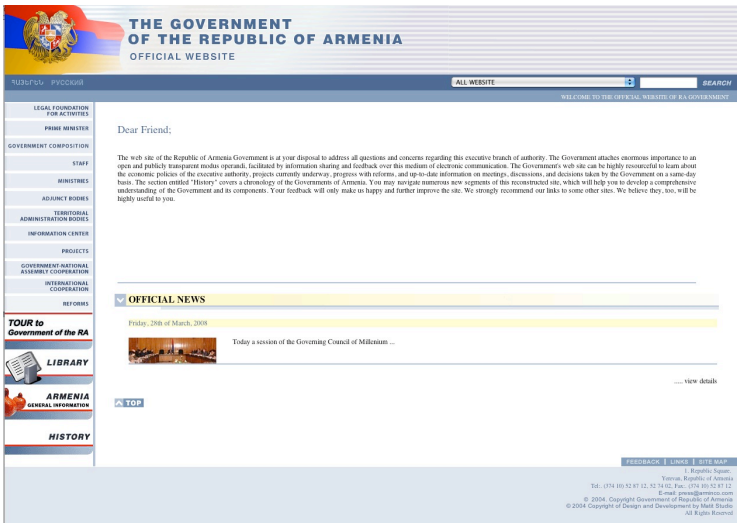


Figure 99: Armenian eGovernment website, source: http://www.gov.am, access on 27.12.2007, 09:23

[882] cf. Europe's Information Society, Political Intelligence Report, Armenia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

The Government of Armenia and the European Commission started an initiative to develop and introduce a pilot system for electronic document circulation and content generation of websites. A computer program allows a multi-user access to different website publication and thus enables the Government decentralizing their publication process by providing each department with the possibility to publish their web content directly.[883]

•ePayment:[884]
Online Payment systems are advanced in Armenia, like payment of utility bills. There are different types of systems in Armenia: the Armenian Card credit card system, the E-Dram prepaid cards system and the International credit cards system:

- The Armenian Card credit card system (ArCa):[885]
  ArCa is the leading local system and was developed with the support of USAID. It is operated by the ArCa Joint Stock Company that was established by large Armenian banks. Initially, the system was used of online payments of public utility bills (like electricity bills), but was later integrated into different websites of web shops for example.
- The E-Dram prepaid cards system:[886]
  This card system is exclusively used for online transactions, especially for people that don‘t have a bank account and use e-commerce for only relatively small transactions. The system is issued in form of prepaid cards or an infomediary financial service, providing only a payment mechanism for a virtual transfer of money without accumulating or managing it.
- The third system uses international credit cards like Visa or MasterCard, but it is not widely used in the online market although it is accepted by many companies.

•eHealth:
The website www.doctror.am provides services for medical staff, like access to journals, software, diagnostic centers and other online resources. The main page is shown in figure 100.

[883] cf. Europe‘s Information Society, Political Intelligence Report, Armenia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[884] cf. Europe‘s Information Society, Political Intelligence Report, Armenia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[885] for more information see: http://www.arca.am

[886] for more information see http://www.edram.am

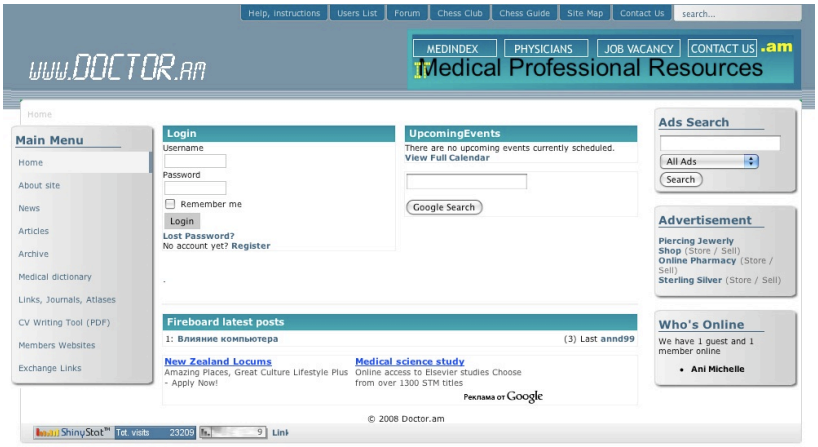


Figure 100: Website www.doctor.am, source: http://www.doctor.am, access on 27.12.2007, 09:37

Another eHealth Service is the Armenian Bone Marrow Registry (http://www.abmdr.am) and the Armenian Medical Association (http://www.armeda.am).

Types of electronic signature

n.a.

4.2.2 Application requirements

Types of certificates

The Armenian e-Science Foundation Certification Authority (see description below), issues certificates that have common fixed components: C=AM, O=ArmeSFo.

The ArmeSFo Certification Authority root certificates include: C=AM, O=ArmeSFo, CN=ArmeSFo CA. The root certificate can be downloaded from http://www.escience.am/ca/cacert.pem.

The ArmeSFo Certification Authority issues certificates for individual users, servers and services and „can be used for:

- e-mail signing and encryption (S/MIME);
- authentication and encryption of communication (SSL/TLS)
- object signing".[887]

More details can be found in the Appendix - Armenia: Extract from ArmeSFo CA - Certificate Policy and Certification Practive Statement.

[887] cf. ArmeSFo CA - Certificate Policy and Certification Practice Statement, Version 0.4, 27 November 2007

Certification Service Providers

➡Short description: The Armenian e-Science Foundation (ArmeSFo) [888]

ArmeSFo was founded in 2002 as a non-governmental and non-profit institution with the goal of introducing, developing and dissemination e-Science technologies in Armenian organizations and scientific centers.

➡Short description: The ArmeSFo Certification Authority[889]

The ArmeSFo Certification Authority was established in 2003 as the first (root level) Certification Authority in Armenia by ArmeSFo, issuing certificates to identify individuals, machines ad services.

The ArmeSFo CA does not issue its certificates to subordinate CAs.

It also serves as a registration authority.

Table 106 lists up all certification service providers in Armenia.

Table 106: Certification Service Provider in Armenia, source: own illustration

Certification Service Provider	Issued Certificates
ArmeSFo Certification Authority	root certificates certificates for individuals and servers (S/MIME, SSL/TLS)

Inspecting authorities

There is no adequate uniform inspecting Authority for electronic information transmission.[890]

4.2.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

n.a.

[888] see http://www.escience.am/

[889] see http://www.escience.am/

[890] cf. Correspondence with Mag. Dina Khvan, commercial attaché for Armenia, Azerbaijan, Belarus, Georgia, Kasachstan, Kirgisistan, Russian Federation, Tadschikistan, Turkmenistan, Usbekistan, Federal Economic Chamber foreign trade office Moskkov

Card readers

All Equipment in context of electronic signatures is supplied by the Russian enterprise Aladin.[891]

Certificate requirements

n.a.

Application programming interface for online-verification

A Certificate Revocation List for the certificates by ArmeSFo CA can be downloads on the site of ArmeSFo, http://armesfoca-crl.fzk.de/crl.pem.

4.2.4 Summary

Table 107 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 107: Summary and rating, Armenia, source: own illustration

categories		rating
legal framework	The area of electronic contracts is not uniquely regulated, there is no specific legislation on eCommerce, In June 2005 a Law on Digital Documents and Digital Signatures has been adopted. lack of accreditation criteria for CSP, only partially adoption of implementing regulations	B
technical standard	cost of computer equipment and connectivity is great obstacle, limited access to electronic communication services due to absence of infrastructure and CSP, eGov in early development stage, not well coordinated, eArmenia initiative in 2003, little progress up to now, only few businesses have own website or use online tools for daily operations or communication and sales, Ministries and governmental authorities have own websites, infrequently updated, containing only general information about institution, no online services, SW certificates, SSL certificates no adequate uniform inspecting authority for electronic information transmission CRL	C
distribution	limited internet access few businesses have own websites with general information, no online tools and services, limited equipment and access to Internet	C

[891] cf. Correspondence with Mag. Dina Khvan, commercial attaché for Armenia, Azerbaijan, Belarus, Georgia, Kasachstan, Kirgisistan, Russian Federation, Tadschikistan, Turkmenistan, Usbekistan, Federal Economic Chamber foreign trade office Moskkov

4.3 Azerbaijan

Figure 101: Fact-sheet: Azerbaijan, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 101 some basic demographic and geographic data of the country is presented.

4.3.1 Institutional frame

Legislation

Azerbaijan concerns about the practical implementation of an e-signature and e-document legislation, particularly regarding how to regulate activities of Certificate Service Providers.

Azerbaijan developed a draft „Electronic Signature Law of the Azerbaijan Republic to adapt international models of digital signature laws on local conditions and compares the legal framework (see Appendix – Azerbaijan: Law on digital electronic signature, Draft). The Draft is tied to public key infrastructure and involves government regulation of signatures and certificate service providers. Furthermore, the Draft centralizes the role of government in the certification process.[892]

At the moment, the Ministry of Communications and Information Technology (MCIT) is trying to learn from experiences of other European countries, particularly from Estonia.

At the beginning of 2006, five legal acts were adopted to clarify and regulate the situation in the country concerning digital signature:

- Rules on Verification of e-signatures,
- Guidelines for registration and Accreditation the centers issuing e-signature certificates and delivering e-signature-related services,
- Guidelines on issuing certificates and maintenance register on e-sign certificates,

[892] cf. Day, Ruth, Comments on Draft „Electronic Signature Law“ of the Azerbaijan Republic, Februar 2002

- Rules on using e-sign in state gov and local gov bodies,
- Guidelines on e-document circulation.[893]

On 12 August 2005 a new „Law on Access to Public Information" entered into force. It was the key to provide more government information vie e-government solutions, by providing interactive official websites and make all relevant data and information available for citizen.

Further regulations about electronic signature can be found in

- the Constitution of the Republic of Azerbaijan
- the Civil Code of the Republic of Azerbaijan
- Law of the Republic of Azerbaijan on Electron Signature and Electron Document, 9.3.2004 (see Appendix - Azerbaijan: Law of the Republic of Azerbaijan on Electron Signature and Electron Document)
- Law of the Republic of Azerbaijan on Electron Trade (see Appendix - Azerbaijan: Law of the Republic of Azerbaijan on Electron Trade)
- Law of the State Secret of the Republic of Azerbaijan.[894]

Availability of online services

•computer availability:

According to the „Communication of Azerbaijan' Statistical Yearbook (for 2005)", the computer penetration lies at 2.3%. The majority of computers are used by public authorities or private companies for clerical work. Computers are used little for private purposes, but the numbers are rising. One reason is the high acquisition costs as a computer is about 3.5 times the average salary (monthly).

•Internet access:

Currently, there are 24 Internet access providers offering a wider range of services in Azerbaijan. Internet connection is dial-up, but in the meantime, also prepaid and post-pard access cards are issued to offer greater choice.

•eGovernment:

Azerbaijan focuses on improving e-commerce and e-governance.

The Azerbaijan internet service market is growing rapidly as the interest of businesses is raising. From 2000 to 2004, the interest growth rate raised about 100 percent.

In 2001, Azerbaijan was the 78th of 133 countries regarding the implementation of eGovernment according to the eGovernment-Global Survey of UNPAN.[895]

---

[893] cf. Europe's Information Society, Political Intelligence Report, Azerbaijan, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[894] cf. Correspondence with Mag. Hans Kausl, commercial attaché for Armenia, Azerbaijan and Georgia and Russia, Federal Economic Chamber, foreign trade office Moscow

[895] The survey can bee accessed under http://www.unpan.org/dpepa-egovernment%20readiness%20report.asp

Azerbaijan established a national e-Governance Network Initiative, the Azerbaijan Government-UNDP Program, in June 2004 to promote building of an Information Society and further transparency of state bodies. The goal of the Government program is to create information portals and access centers which facilitate the interaction between the government and citizens.[896]

A new online tax system went recently online. Citizen can register their tax returns and pay taxes directly[897].

•ePayment:
The banking sector has pushed e-payment systems by introducing credit cards and online payment systems. For example, an electronic payment system was launched that allows the transfer of money between cardholders and also non-cardholders: CONTACT.[898] It is one of the largest systems operating.[899]
Also a 2005-2007 State Programme on the Implementation of a National e-Payment System was set up, involving a range of different e-payment innovations. The planned operations can be observed in detail in the Appendix - Azerbaijan: 2005-2007 State Program on the Implementation of a National e-Payment System.[900]

•eHealth:[901]
There are only little online health resources offered online, like http://doctor.aznet.org or http://www.mednet.az, but there are only quite basic. Both platforms are displayed in the figures 102 and 103.

[896] cf. Europe's Information Society, Political Intelligence Report, Azerbaijan, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[897] cf. Europe's Information Society, Political Intelligence Report, Azerbaijan, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[898] cf. Europe's Information Society, Political Intelligence Report, Azerbaijan, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[899] cf. Rabita Dunyasi, International Bank of Azerbaijan started operations in „Contact" system, press release, http://www.rabitadunyasi.info.az/rd/dim.asp?id=3353, access on 28.12.2007, 18:52

[900] cf. 2005-2007 State Program on the Implementation of a National e-Payment System, http://www.nba.az/download/o_sistemi/dprengimpl.xls, access on 28.12.2007, 18:59

[901] cf. Europe's Information Society, Political Intelligence Report, Azerbaijan, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

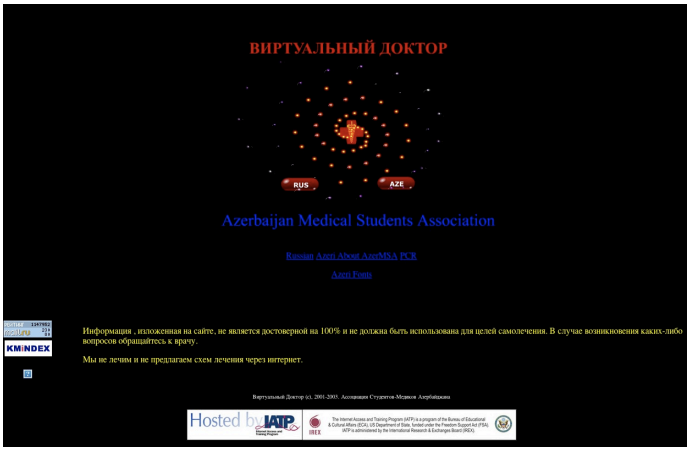


Figure 102: doctor.aznet.org, source: http://doctor.aznet.org, access on 28.12.2007, 19:24

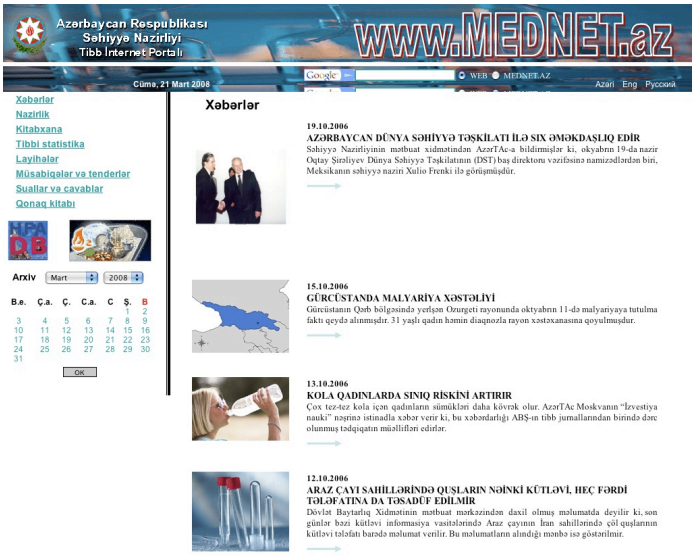


Figure 103: mednet.az, source: http://www.mednet.az,access on 28.12.2007, 19:28

Types of electronic signature

n.a.

4.3.2 Application requirements

Types of certificates

n.a.

Certification Service Providers

n.a.

Table 108 lists up all certification service providers in Azerbaijan.

Table 108: Certification Service Provider in Azerbaijan, source: own illustration

Country	Certification Service Provider	Issued Certificates
Azerbaijan	n.a.	n.a.

Inspecting authorities

Actually, no independent National Regulatory Authority exists in Azerbaijan. The basic regulation functions are executed by the Ministry of Communications and Information Technology (MICT).

➡short description: MICT

The Ministry of Communications and Information Technologies was brought into being in February 2004. It was intended to assume a regulatory function and established as a „high-level policy body within the Government, responsible for promoting the development of the ICT sector, by creating a favorable regulatory environment and monitoring the implementation of ICT projects nationwide.“[902]

4.3.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

n.a.

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

[902] cf. Europe‘s Information Society, Political Intelligence Report, Azerbaijan, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

4.3.4 Summary

Table 109 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 109: Summary and rating, Azerbaijan, source: own illustration

categories		rating
legal framework	2002: Azerbaijan adopted a draft „Electronic Signature Law“ to adapt international models of digital signature laws on local conditions. At the beginning of 2006, 5 legal acts have been adopted to clarify and regulate the situation in the country concerning digital signature,	A
technical standard	little computer penetration, high acquisition costs of computers, most are used by public authorities or private companies focus on improving eCommerce and eGovernment, eGovernance Network Initiative eTax system eHealth: only little health resources, quite basic no independent national Regulation Authority	C
distribution	little computer penetration, high costs of equipment	C

4.4 Bosnia and Herzegovina

Figure 104: Fact-sheet: Bosnia and Herzegovina, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 104 some basic demographic and geographic data of the country is presented.

4.4.1 Institutional frame

Legislation

Electronic Signatures are regulated by the Law for electronic Signature official register Bosnia and Herzegovina No. 91/06.[903]

Availability of Online Services

•eGovernment:

Recently, Information and Communication Technology (ICT) began to receive attention and turned into an important factor in long-term development of the state. ICT plays an important role for the interaction between business, government and citizens. It is a key sphere of government: It was identified as a priority and written down in the „e-Agenda" document in 2002. But Bosnia and Herzegovina is in a difficult economic and political situation, therefore, the topic of ICT and eGovernment has remained isolated so far.

But the country started several initiatives lately:

- June 2002: Information Society policy paper, adopted by Council of Ministers,

[903] cf. Correspondence with Mag. Astrid Pummer, commercial attaché for Bosnia and Herzegovina, Federal Economic Chamber foreign trade office Sarajevo

- May 2003: ICT Forum, supported by the United Nations Development Programme (UNDP)[904],
- Memorandum of Understanding between Government and UNDP concerning outlining and responsibilities in developing the ICT Strategy.[905]

Types of electronic signature

n.a.

4.4.2 Application requirements

Types of certificates

n.a.

Certification Service Providers

Currently there is no Authority to certify electronic Signatures in Bosnia and Herzegovina.[906]

Table 110 lists up all certification service providers in Bosnia and Herzegovina.

Table 110: Certification Service Provider in Bosnia and Herzegovina, source: own illustration

Certification Service Provider	Issued Certificates
no CSP	-

Inspecting authorities

n.a.

4.4.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

n.a.

[904] for more information see http://www.undp.ba/

[905] cf. UNDP, United Nations Development Programme and the Government of Bosnia and Herzegovina, Development of BiH ICT Strategy, Preparatory Assistance Document, 1.7.2003

[906] cf. Correspondence with Mag. Astrid Pummer, commercial attaché for Bosnia and Herzegovina, Federal Economic Chamber foreign trade office Sarajevo

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

4.4.4 Summary

Table 111 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 111: Summary and rating, Bosnia and Herzegovina, source: own illustration

categories		rating
legal framework	Electronic signatures are regulated by the Law for electronic signature official register Bosnia and Herzegovina No. 91/06.	A
technical standard	Bosnia is in difficult economic and political situation, therefore topics eGovernment and ICT have remained isolated so far, lately some ICT initiatives no authority to certify electronic signatures	C
distribution	no eGov, no ICT, no authority	C

4.5 Georgia

Figure 105: Fact-sheet: Georgia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 105 some basic demographic and geographic data of the country is presented.

4.5.1 Institutional frame

Legislation

Since December 2000, Georgia has created five draft laws on e-commerce, concerning e-documents, electronic signatures, verification and numerous other e-commerce issues (see Appendix - Georgia: Electronic Records and Signatures Act).

The draft laws also list up requirements for digital signature providers.[907]

Availability of online services

•eGovernment as not taken off in Georgia yet because of less Internet penetration in the county.

eCommerce is not common in Georgia. Only one out of three businesses have an own website.

Also the majority of Georgian ministries don‘t have websites, existing webpages only contain little information.

But Georgia has started some initiatives to digitize documents, for example documentation of the Ministry of Telecommunication in 2003, but there are little results until now.

•eHealth:

The Georgian Telecedicine Union[908] is promoting eHealth actively in Georgia and developed a proposal for creating a national e-health network. However, it has not been implemented until now.

[907] cf. Europe‘s Information Society, Political Intelligence Report, Georgia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[908] see http://georgia.telepathology.org

•ePayment:[909]

ePayment systems are not widely spread in Gerorgia. There is also no comprehensive regulatory framework. However, some services are starting to appear, for example, the TBC bank was quite active in different international projects. In 1996, the bank joined Swift (www.swift.com). Integrated in the „Visa Electron credit card system", the bank provides a range of basic online services like offering phone cards, utility bill paying and account status operations.

To provide innovative electronic services for payment card customers, TBC bank cooperates with Intellectbank and UFC International (https://secure.ufc.ge/index.php) and offers different services, for examples SMS-based services that enable to block or unblock their cards of pay for phone services.

Types of electronic signature

n.a.

4.5.2 Application requirements

Types of certificates

n.a.

Certification Service Providers

The ICT department of the Georgian Ministry of Economic Development is in charge of issuing digital signatures.[910]

Table 112 lists up all certification service providers in Georgia.

Table 112: Certification Service Provider in Georgia, source: own illustration

Country	Certification Service Provider	Issued Certificates
Georgia	Ministry of Economic Development, ICT department	n.a.

Inspecting authorities

n.a.

[909] cf. Europe's Information Society, Political Intelligence Report, Georgia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[910] cf. Europe's Information Society, Political Intelligence Report, Georgia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

4.5.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

n.a.

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

4.5.4 Summary

Table 113 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 113: Summary and rating, Georgia, source: own illustration

categories		rating
legal framework	Georgia has created five draft laws on eCommerce, concerning eDocuments, electronic signatures, verification, requirements for CSP etc	A
technical standard	little Internet penetration, no eGov, no eCommerce, majority of Ministries don‘t have own websites, only 1/3rd of businesses have own website, Georgia started some initiatives to digitalize documents, but with little results	C
distribution	little Internet penetration, no eGov, no eCommerce, majority of Minitries don‘t have own websites	C

4.6 Iceland

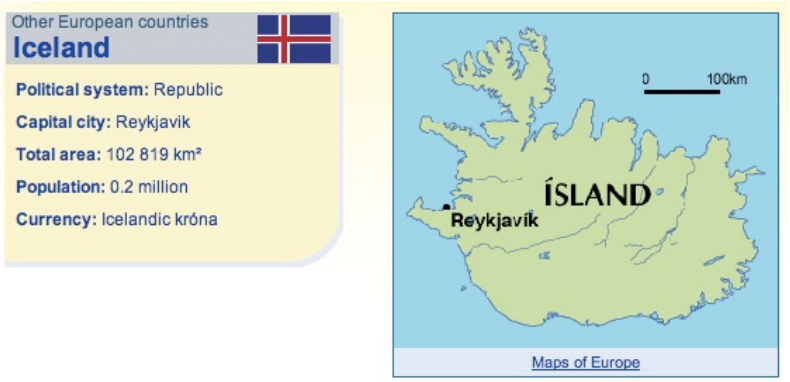


Figure 106: Fact-sheet: Iceland, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:55

In figure 106 some basic demographic and geographic data of the country is presented.

4.6.1 Institutional frame

Legislation

In April 2001, an act on qualified electronic signatures is passed (see Appendix – Iceland: E-Commerce Act).

Availability of Online Services

•eGovernment:

Iceland was the first country in the world that became digitalized in 1995.[911]

Digital signatures play an important role in building up confidence in e-governmental services. The aim is to enable that every citizen can obtain a digital certificate and other equipment to create a digital signature and encrypt data and information.

According to information from Eurostat, Iceland is one of Europe's leading countries in E-government: 68% of Icelanders uses the internet to obtain information from public authorities, 36% downloads forms and 23% sends completed forms over the internet.[912]

[911] cf. Ministry of Communications, Iceland

[912] cf. Eurostat (2005)

Types of electronic signature

Currently, only basic electronic signature is available, but Iceland hopes to provide secure electronic signature before the end of this year.[913]

4.6.2 Application requirements

Types of certificates

In Iceland, certificates from VeriSign are dominant. VeriSign is represented by Skyrr.

Certification Service Providers

There is only one CSP in Iceland, and it is not accredited yet.[914]

VeriSign is represented by Skyrr.[915]

Table 114 sums all certification service providers in Iceland.

Table 114: Certification Service Provider in Iceland, source: own illustration

Certification Service Provider		Issued Certificates
Skyrr	Skyrr	n.a.

Inspecting authorities

The Body responsible for supervision of CSPs is Neytendastofa, the Consumer Agency.

➡Short description: Neytendastofa[916]

The Consumer Agency was established 1 July 2005 according to Act No 62/2005 (also available in Danish). The Consumer Agency is one of the governmental agencies in Iceland which is entrusted with market surveillance of business operators, good functioning and transparency of the markets in respect to safety and consumers legal rights as well as enforcement of legislation adopted by the Icelandic Parliament for protection of consumers health, legal and economical rights.

The Consumer Agency is a governmental agency falling under the auspices of Ministry of Trade.

[913] cf. Correspondence with Grimur Kjartansson, Neytendastofa, The Consumer Agency, Iceland

[914] cf. Correspondence with Grimur Kjartansson, Neytendastofa, The Consumer Agency, Iceland

[915] cf. Correspondence with Grimur Kjartansson, Neytendastofa, The Consumer Agency, Iceland

[916] cf. Correspondence with Grimur Kjartansson, Neytendastofa, The Consumer Agency, Iceland

4.6.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

- E-ID card:

By 2007, Governments tries to equip every citizen with en electronic ID, on a smartcard. The eIDs can be used for governmental services, where authentication and digital signature is required.

The Consumer Agency recommends those signature-creation devices that are conform to the Cen Workshop Agreement - CWA 14172-5 (see Appendix – Iceland: Cen Workshop Agreement - CWA 14172-5).[917]

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

4.6.4 Summary

Table 115 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 115: Summary and rating, Iceland, source: own illustration

categories		rating
legal framework	The EU-directive on Electronic Signatures was implemented in 2001.	A
technical standard	eGovernment: Iceland was the first country that became digitized in 1995, eSignature has important role building up confidence in eGov services. currently only basic electronic signature, hope to provide secure eS by the end of this year, only one CSP, not accredited By 2007, Government tries to equip citizens with eID on smartcard.	C
distribution	Iceland is one of Europe's leading countries in eGovernment, 23% of Iceland's citizens send forms complete electronically to public authorities no statistics on use of electronic signature	-

[917] cf. Correspondence with Grimur Kjartansson, Neytendastofa, The Consumer Agency, Iceland

4.7 Moldova

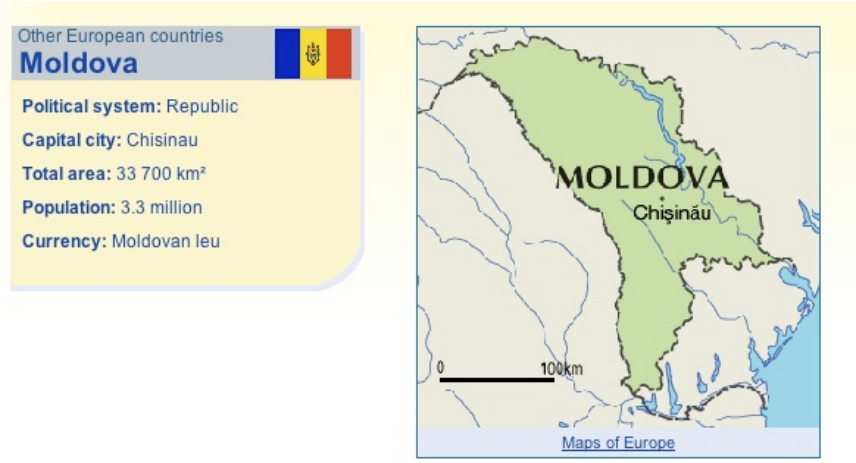


Figure 107: Fact-sheet: Moldavia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 107 above some basic demographic and geographic data of the country is presented.

4.7.1 Institutional frame

Legislation[918]

In 2004, two key laws have been adopted:

- Law of the Republic of Moldova on Electronic Documents and the Electronic Signature
- Law of the Republic of Moldova on Electronic Commerce.

According to the laws, electronic documens have same legal power and value as paper documents..

Three further regulations were approved in 2006:

- Regulation of the Centre for Certification of High Level Public Keys
- Regulation Regarding the Procedure of Registration of the Centres for Certification of Public Keys
- Special Conditions for the Activity of Centres for Certification of Public Keys.

[918] cf. Europe's Information Society, Political Intelligence Report, Moldova, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

Availability of Online Services

•Computer Availiability:[919]

Only 10.2 % of Moldavian households have a personal computer (347.991 computers in 2005), 28% have access to a computer.

9.9% of employees in Moldova use a computer (in 2004 52.540 computers, 42.385 networked)

•Internet access:[920]

The total number of Internet connections in 2005 was 223.224. For connection, broadband, xDSL and dial-up connection is used. ADSL is predominant.

The number of Internet users is increasing from year to year (406.000 users in 2004), thanks to new service providers, public internet access centers and connections form schools.

48.8 % of all Moldavian companies have internet access.

•eCommerce:[921]

eCommerce is in an early development phase in Moldova. A survey on the circulation of eDocuments showed that:

- 30.1% received orders via Internet
- 36.5% accessed public agengies‘ websites
- 40% of companies using Internet have their own homepage
- 23.1% obtained electronic information.

Over 3.370 Websites do exist in Moldova, 52% only available in Romanian, 21% in Romanian, Russian and English.

Also government institutions have their own websites offering information (70% in Russian, 30% in English).

•eGovernment:

67% of all public insittutions in Moldova offer online information concerning their services and activities.[922]

Moldova is keen in improving information society and declared the erection as one of the national priorities in 2004. A project E-Moldova was started that focuses on the following areas of invention:

- electronic readiness
- new National Strategy
- Action Plan for Information Society Technologies for Development.[923]

---

[919] cf. Europe‘s Information Society, Political Intelligence Report, Moldova, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[920] cf. Europe‘s Information Society, Political Intelligence Report, Moldova, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[921] cf. Europe‘s Information Society, Political Intelligence Report, Moldova, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[922] cf. Europe‘s Information Society, Political Intelligence Report, Moldova, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[923] cf. UNDP Moldova, Focus Areas, http://www.undp.md/focus_areas/projects/stories/ict.shtml, access on 03.01.2008, 14:12

The Moldavian Government elaborates with support of UNDP a strategy for E-Moldova and a concept for eGovernment.[924]

The creation of an national information society shall improve quality of live and contribute to a community development in Moldova.[925]

Types of electronic signature

n.a.

4.7.2 Application requirements

Types of certificates

n.a.

Certification Service Providers

In 2006, the first „Public Key Certification Center" was opened by CST, the Centre for Special Teleommunications, issuing keys to public servants of public administrative institutions.

Table 116 lists up all certification service providers in Moldova.

Table 116: Certification Service Provider in Moldova, source: own illustration

Certification Service Provider	Issued Certificates
n.a.	n.a.

Inspecting authorities

n.a.

4.7.3 Technical preconditions

Signature Software

n.a.

[924] cf. UNDP Moldova, Advancing e-Government Solutions for Friendly, Efficient and Secure Public Service, Press Release, April 24, 2007, http://www.undp.md/presscentre/2007/bit+.shtml, access on 03.01.2008, 14:16

[925] cf. UNDP Moldova, Focus Areas, http://www.undp.md/focus_areas/projects/stories/ict.shtml, access on 03.01.2008, 14:12

Types of secure signature-creation device

n.a.

Card readers

n.a.

Software certificate requirements

n.a.

Application programming interface for online-verification

n.a.

4.7.4 Summary

Table 117 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 117: Summary and rating, Moldova, source: own illustration

categories		rating
legal framework	2004: Law on Electronic Documents and Electronic Signature, Law on eCommerce 2006: further regulations on public keys	A
technical standard	keen on improving information society, eMoldova project started to provide electronic readiness	C
distribution	project to provide electronic readiness, no eGov yet	C

4.8 Monaco

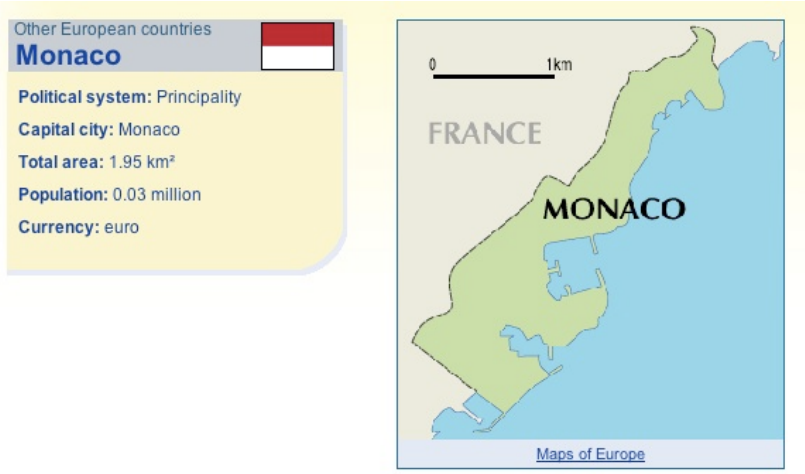


Figure 108: Fact-sheet: Monaco, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 108 some basic demographic and geographic data of the country is presented.

4.8.1 Institutional frame

Legislation

n.a.

Availability of Online Services

•eGovernment:

The Brown University of America has surveyed international eGovernment projects and stated, that Monaco is under the top countries concerning the offer of electronic information and services.[926]

Types of electronic signature

n.a.

[926] cf. Deborah Asbrand, E-Government: Kleine Länder groß im Internet, Press release, Heise.de, Technology Review, 7.10.2004, http://www.heise.de/tr/E-Government-Kleine-Laender-gross-im-Internet--/artikel/51935, access on 03.01.2008, 14:39

4.8.2 Application requirements

Types of certificates

n.a.

Certification Service Providers

n.a.

Table 118 lists up all certification service providers in Monaco.

Table 118: Certification Service Provider in Monaco, source: own illustration

Certification Service Provider	Issued Certificates
n.a.	n.a.

Inspecting authorities

n.a.

4.8.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

n.a.

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

4.8.4 Summary

Table 119 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 119: Summary and rating, Monaco, source: own illustration

categories		rating
legal framework	-	-
technical standard	Monaco is under the top countries concerning the offer of electronic information and services no information about eS	-
distribution	-	-

4.9 Montenegro

Figure 109: Fact-sheet: Montenegro, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 109 some basic demographic and geographic data of the country is presented.

4.9.1 Institutional frame

Legislation

A Law on Electronic Signature has been adopted and drafts are in preparation:

- draft Law on Electronic Trade
- rules about evidence, register and obliged insurance of certificated service deliverers,
- rules about measures and procedure of using and protecting electronic signature and certification systems,
- rules about technical policies and conditions of connecting the system of certificated electronic signature.[927]

The law on electronic signatures can be found in the Appendix - Montenegro: Electronic Signature Law.[928]

In May 2005, the Law on Amendments and Supplements on the Electronic Signature Law was adopted.

---

[927] cf. MIPA, Electronic Signature Law, http://www.mipa.cg.yu/pdf/zakoni/Electronic%20Signature%20Law.pfd , access on 09.01.2008, 08:46

[928] cf. http://www.mipa.cg.yu/pdf/zakoni/Electronic%20Signature%20Law.pdf, access on on 09.01.2008, 08:54

Availability of Online Services[929]

Moldova started a „Strategy of Development of Electronic Communications) and defined key priorities for the eGovernment stategy until 2008:

- implementation of regulations
- single and secure internet network with all government and local bodies
- Operation of public Internet access points
- Building an Information System for administrative procedures

Types of electronic signature

n.a.

4.9.2 Application requirements

Types of certificates

n.a.

Certification Service Providers

n.a.

Table 120 lists up all certification service providers in Montenegro.

Table 120: Certification Service Provider in Montenegro, source: own illustration

Certification Service Provider	Issued Certificates
n.a.	n.a.

Inspecting authorities

n.a.

4.9.3 Technical preconditions

Signature Software

n.a.

[929] cf. Milo Djukanovic, Prime Minister of the Republic of Montenegroat the Microsoft Government Leaders Forum, http://www.vlada.cg.yu/eng/premijer/index.php?akcija=vijesti&id=10828 , access on 09.01.2008, 09:02

Types of secure signature-creation device

n.a.

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

4.9.4 Summary

Table 121 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 121: Summary and rating, Montenegro, source: own illustration

categories		rating
legal framework	Law on Electronic Signature adopted 2003, some drafts in preparations	A
technical standard	no eGov, stratgegy of development of electronic communications eGovernment: key priorities until 2008	C
distribution	no eGov	C

4.10 Norway

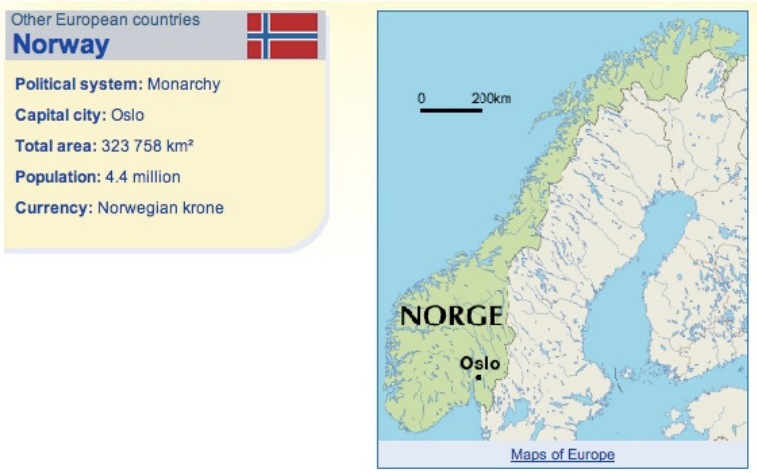


Figure 110: Fact-sheet: Norway, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:56

In figure 110 some basic demographic and geographic data of the country is presented.

4.10.1 Institutional frame

Legislation

The Norwegian Government passed the Electronic Signature Act that went into force in July 2001. (see Appendix – Norway: Electronic Signature Act).

•recognition of foreign certificates:[930]

In March 1998, the agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:

Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

The primary agreement of reciprocal acceptance of IT security certificates on basis of the Common Criteria up to the evaluation grade EAL4 was signed in October 1998 between France, Germany, Great Britain, Canada and the USA. Currently (status June 2006) 24 STates have joined the Common Criteria Mutual Recognition Agreement:

- Australia,Germany, France Japan, Canada, Netherlands, New Zealand, Norway, South Korea, USA joined as Certificate Authorizing Participants,
- Denmark, Finland, Greece, India, Israel, Italy, Austria, Sweden, Singapore, Spain, Czech Republic, Turkey and Hungary as Certificate Consuming Participants.

[930] cf. Study of the Donau Universität Krems, Master-Studie, Austria

Availability of Online Services

•eGovernment:

Norway is very engaged to make government more efficient and service-oriented. Therefore the eNorway 2009 project was launched in June 2005. The target was to build a PKI to enable a secure communication within the government and with citizens and companies via electronic public services offered on the Internet. A Portal has been developed and some key services have been launched, like support services or interactive maps.

To access these services, the Norwegian public administration supports the use of smart cards.

The Norwegian eGovernment is coordinated by the Norwegian Ministry of Modernization.[931]

Types of electronic signature

n.a.

4.10.2 Application requirements

Types of certificates

n.a.

Certification Service Providers

n.a.

Table 122 lists up all certification service providers in Norway.

Table 122: Certification Service Provider in Norway, source: own illustration

Certification Service Provider	Issued Certificates
n.a.	n.a.

Inspecting authorities

The Body responsible for supervision is the Norwegian Post and Telecommunications Authority.

➡Short description: Norwegian Post and Telecommunications Authority (NPT)[932]

NTP is an self-financed administrative agency under the control of the Norwegian Ministry of Transport and Communications that is responsible for the telecommunications market in Norway.

[931] cf. http://ec.europa.eu/information_society/activities/egovernment_research/countries/norway/index_en.htm, access on 06.08.07, 11:49

[932] cf. http://www.npt.no/portal/page/portal/PG_NPT_NO_EN/PAG_NPT_EN_HOME/PAG_ABOUT/PAG_ORGANIZATION?menuid=11798 , access on 06.08.07, 11:17

4.10.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

About 300000 electronic ID cards have been issued until 2005. The card costs 10€ and is valid for 3 years. Currently, 10 services are available and can be used with the card: Lottery, NetBank, Social Security, Student loan agreement etc.

Further, a multi-application card is used: with electronic wallet and electronic signature.[933]

Card readers

n.a.

Software certificate requirements

n.a.

Application programming interface for online-verification

n.a.

4.10.4 Summary

Table 123 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 123: Summary and rating, Norway, source: own illustration

categories		rating
legal framework	The EU-directive on Electronic Signatures was passed in 2001.	A
technical standard	In 2005, eGovernment was launched: eNorway 2009, use of smartcards eID card for electronic services multi-application card with electronic wallet and electronic signature	B
distribution	About 300.000 electronic ID cards have been issued until 2005, no statistics on use of electronic signature	-

[933] cf. http://www.libertysecurity.org/article511.html, access on 01.08.2007, 23:59

4.11 Russia

Figure 111: Fact-sheet: Russia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 111 some basic demographic and geographic data of the country is presented.

4.11.1 Institutional frame

Legislation

Electronic Signatures were not regulated by law for many years. In 2002, the Federal Law on Electronic Digital Signatures was passed, the Russian Federation Federal Law on Electronic Signatures (see Appendix - Russia: Draft Law on Electronic Signatures).

The law governs the following principles:

- electronic signature is recognized equivalent to handwritten signature,
- government supervises commerce concerning eSignature,
- Information systems are divided into common-use and corporate systems, depending on degree of governmental supervision.[934]

•recognition of foreign certificates:

Foreign certificates are recognized in Russia if they are authenticated under the foreign law and observed under the Russian law for recognition of legal effect.[935]

[934] cf. Naumov, Victor, Nikiforova, Tatiana, Electronic signatures in Russian law, The e-Signature Law Journal, December 2005, http://www.e-signaturelawjournal.co.uk, access on on 10.01.2008, 10:40

[935] cf. Naumov, Victor, Nikiforova, Tatiana, Electronic signatures in Russian law, The e-Signature Law Journal, December 2005, http://www.e-signaturelawjournal.co.uk, access on 10.01.2008, 10:40

Availability of Online Services

•Computer availability:[936]

In 2006, the number of computers was 17.4 million in households, which means 26 computers/100 households. The cost for a computer is very high and unaffordable for many households. There are very few computer owners in Russia.

•eCommerce: [937]

In 2006, only 16.9% of businesses have their own website. This is a great obstacle for the development of eCommerce. Those who have a website use internet to provide general information (24.9%), to receive online orders (16.3%9 or to manage customer relationships (9.9% eSettlements, 3.0% after-slates services).

•eGovernment:

One big obstacle is that only 27.6% of federal authorities, 24.2% of regional authorities and 4.6% of local authorities have their own website.[938]

In 2001, Russia launched Electronic Russia, promoting Internet, e-Commerce and Electronic Education. Governmental agencies should be more transparent and open their information to the public.[939]

The eRussian programme focuses on ICT usage by authorities to boost the use of Internet websites.[940]

The Government wants to make official information accessible by using IT.

So far, an eGovernmental portal was created: http://www.government.ru (figure 112). Also several regions participate in pilot programs of implementing eGovernment solutions including electronic mail and document management systems.

---

[936] cf. Europe‘s Information Society, Political Intelligence Report, Russia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[937] cf. Europe‘s Information Society, Political Intelligence Report, Russia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[938] cf. Europe‘s Information Society, Political Intelligence Report, Russia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[939] cf. Economist Intelligence Unit, Russia: Overview of e-commerce, 05.December 2006, Article in Global Technology Forum, http://globaltechforum.eiu.com/index.asp?layout=rich_story&doc_i…title=Russia%3A+Overview+of+e-commerce&channelid=4&categoryid=29, access on 10.01.2008, 10:25

[940] cf. Europe‘s Information Society, Political Intelligence Report, Russia, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

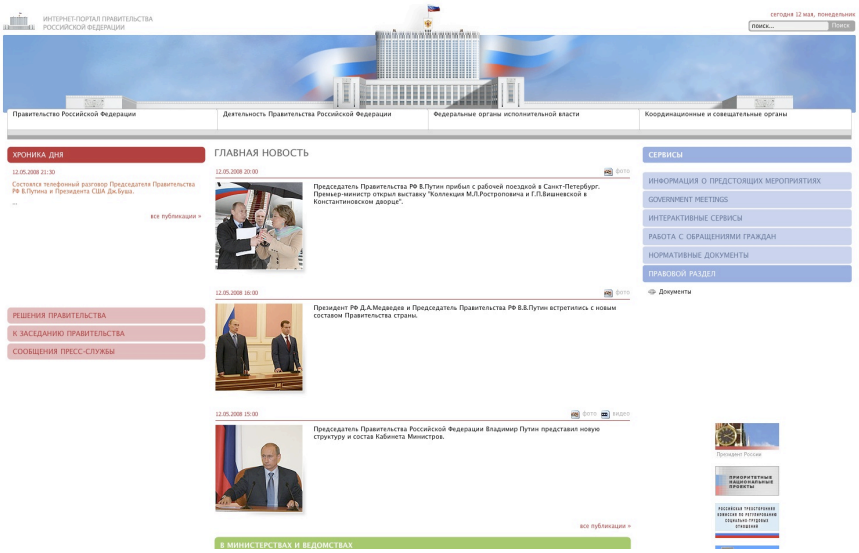


Figure 112: eGovernment portal, source: http://www.government.ru/content/, access on 10.01.2008, 12:44

In 2001, online usage of government was only 3%. The goal of government is that electronic interactions will number 65% of communication (internal) and 40% of communication between institutions by 2010.

Electronic documents are more and more used in Russia for business purposes.[941]

Types of electronic signature

n.a.

4.11.2 Application requirements

Types of certificates

n.a.

Certification Service Providers

n.a.

Table 124 lists up all certification service providers in Russia.

Table 124: Certification Service Provider in Russia, source: own illustration

Certification Service Provider	Issued Certificates
n.a.	n.a.

[941] cf. Naumov, Victror, Nikiforova, Tatiana, Electronic signatures in Russion Law, The e-Signature Law Journal, December 2005, http://www.e-signaturelawjournal.co.uk, access on 10.01.2008, 10:40

Inspecting authorities

n.a.

4.11.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

n.a.

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

n.a.

4.11.4 Summary

Table 125 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 125: Summary and rating, Russia, source: own illustration

categories		rating
legal framework	Federal Law on Electronic Signature was passed in 2002.	A
technical standard	In 2006, only 16.9% of businesses have their own website, great obstacle for the development of eCommerce 2001: eRussia to promoting Internet, e-Commerce and Electronic Education, Governmental agencies should be more transparent and open their information to the public, focus on ICT usage by authorities to boost the use of Internet websites	C
distribution	In 2006, the number of computers was 17.4 million in households, which means 26 computers/100 households. The cost for a computer is very high and unaffordable for many households. There are very few computer owners in Russia In 2006, only 16.9% of businesses have their own website use of eGov in 2001: only 3%, no statistics about electronic signature	C

4.12 Serbia

Figure 113: Fact-sheet: Serbia, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 113 some basic demographic and geographic data of the country is presented.

4.12.1 Institutional frame

Legislation

Electronic signature Law was ratified in Serbia in December 2004. Unfortunately, the Law is still not being enforced. Enforcement of the Law is expected to start until the end of this month by first accreditations of Certification Authorities (CA).[942]

Decrees that define electronic signature in detail are passed not until 10.3.2008. It was announced, that the law will be adopted in summer 2008. In the Appendix - Serbia: Laws on electronic signature the laws can be found but only a Serbian Version was available.[943]

[942] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

[943] cf. Correspondence with Dr. Herbert Preclik, commercial attaché for,Kosovo, Mazedonien, Montenegro, Serbien, Federal Economic Chamber, foreign trade office Belgrad, and Mag. Nebojsa, assistent minister for IT, Ministry for Telecommunication and Information Society, Republic of Serbia

Availability of Online Services

•eGovernment:

At the beginning of 2007, a central portal for eGovernment services was created by the National Internet and Information Technology Agency. The goals include the implementation of one access point for electronic government services and Access to basic services for citizen, businesses and public administration.[944] The design of the portal is shown in figure 114.

Figure 114: eGovernment Portal Serbia, source: http://www.euprava.gov.yu/, access on 11.01.2008, 08:15

•eIdentification:

The first prerequisite was the Law on Electronic Signature that was adopted in 2004. But due to the absence of many laws (like a law on Personal Data Protection), no national certification body is offering its services yet.

In 2001, the project eCards started but had to face some barriers like technical problems or other requirements (legal, infrastructure,...). In 2006, the Law on Personal Cards was released and citizens can now choose between standards or electronic personal cards. But before the cards can be used, the Law on DAta Protection must be adopted.[945]

[944] cf. Babovic, Zoran, Darko, Jovic, Milutinovic, Velijko, Survey of eGovernment Services in Serbia, 26 August 2007, Informatica 31 (2007) 379-396

[945] cf. Babovic, Zoran, Darko, Jovic, Milutinovic, Velijko, Survey of eGovernment Services in Serbia, 26 August 2007, Informatica 31 (2007) 379-396

Types of electronic signature

In Serbia, two kinds of electronic signature are existing: qualified (SSCD) signature and non-qualified signature.[946]

Electronic signature is being used just a little in Serbia at this moment, and when it is used, it is usually advanced electronic signature.[947]

4.12.2 Application requirements

Types of certificates

At this moment, just advanced electronic certificates are used, both hardware and software. As mentioned in previous clause, qualified electronic certificates will exist when first CA accreditations occur.[948]

Qualified certificates must be issued by a certification agency. Currently, no agency exists because the requirements that such an agency must fulfill will be passed not until March 2008. The certificates will be defined after the Formats for documents ETSI TS 101 862, RFC 3739 and ETSI TS 102 280.[949]

The Post Serbia Certification Authority issues four categories of digital certificates:

- WEB certificates: x.509 version 3 certificate, use with Microsoft applications,
- SID Enterprise certificates (single application ID): x.509 version 3 certificate, use with Entrust applications and Microsoft applications
- MID Enterprise certificates (multiple application ID): x.509 version 3 certificate, use with Entrust applications and Microsoft applications
- SER certificates for Web Server: x.509 version 3 certificate, configuration of SSL, TLS protocols on web servers and clients.[950]

---

[946] cf. Correspondence with Dr. Herbert Preclik, commercial attaché for,Kosovo, Mazedonien, Montenegro, Serbien, Federal Economic Chamber, foreign trade office Belgrad, and Mag. Nebojsa, assistent minister for IT, Ministry for Telecommunication and Information Society, Republic of Serbia

[947] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

[948] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

[949] cf. Correspondence with Dr. Herbert Preclik, commercial attaché for,Kosovo, Mazedonien, Montenegro, Serbien, Federal Economic Chamber, foreign trade office Belgrad, and Mag. Nebojsa, assistent minister for IT, Ministry for Telecommunication and Information Society, Republic of Serbia

[950] cf. http://www.cepp.co.yu/ca/english.asp, access on 11.01.2008, 08:23

Certification Service Providers

At this moment, Post Serbia is the only public CA.[951] Since 16.11.2004 it issues digital certificates to individuals as well as to legal entities.[952]

There are internal CAs in some banks and companies.
At this moment, there is no accredited CA.[953]

Table 126 lists up all certification service providers in Serbia.

Table 126: Certification Service Provider in Iceland, source: own illustration

Certification Service Provider		Issued Certificates
Post Serbia	Post Serbia Certification Authority	WEB certificate SID / MID Enterprise certificate SER Web server certificate

Inspecting authorities

The Ministry of Telecommunication and Information Society observes the Certification Authority.[954]

4.12.3 Technical preconditions

Signature Software

n.a.

Types of secure signature-creation device

Post Serbia recommends PKI smart cards and PKI USB smart tokens with EAL 4+ (preferred) or FIPS 140-3 Level 2 or higher certification.[955]

[951] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

[952] cf. Babovic, Zoran, Darko, Jovic, Milutinovic, Velijko, Survey of eGovernment Services in Serbia, 26 August 2007, Informatica 31 (2007) 379-396

[953] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

[954] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

[955] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

Card readers

For desktop computers, Post Serbia CA recommends desktop readers with USB interface. Post Serbia has never used PIN-entry readers.[956]

Certificate requirements

For creation of signature, some kind of software is required. Post Serbia, as a CA, does not provide any software. Software and operating system are chosen by end users.[957]

For software certificates, the user must have installed Microsoft Internet Explorer or Mozilla Firefox.[958]

Application programming interface for online-verification

Post Serbia provides a certification revocation list for online verification, but no online certificate status protocol.[959]

4.12.4 Summary

Table 127 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 127: Summary and rating, Serbia, source: own illustration

categories		rating
legal framework	Electronic signature law was ratified in Serbia in December 2004, but the law is not enforced yet, It was anncounced that the law wiill be adopted in Summer 2008, absence of other laws like on personla data protection no requiremens exist for agency to issue qualified certificates	C
technical standard	eGovernment, no national certification body is offering its services for eldentification eID card project had to face some barriers like technical problems and other requirements qualified electronic signature on secure signature creation device non qualified electronic signature advanced electronic certificates, both hardware and software smartcard, token no agency that issues qualified certificates set that an agency must fulfill only one CSP, not accredited CRL	B
distribution	electronic signature is used little	C

[956] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

[957]cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

[958] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

[959] cf. Correspondence with Dragan Spasic, Manager for digital certificates, Post Serbia

4.13 Switzerland

Figure 115: Fact-sheet: Switzerland, source: http://europa.eu/abc/european_countries/index_en.htm, access on 28.02.08, 14:45

In figure 115 some basic demographic and geographic data of the country is presented.

4.13.1 Institutional frame

Legislation

Switzerland was one of the first countries in Europe to recognize electronic signatures.
A law was approved in the House of Representatives.

On the 1st January 2005, the Federal law on certification services within the scope of the electronic signature (ZertES, SR 943.03) (see Appendix - Switzerland: Federal law on certification services within the scope of the electronic signature) came into force.
At the same time, the Ordinance on certification services within the scope of the electronic signature (VZertES, SR 943.032) (see Appendix - Switzerland: Ordinance on certification services within the scope of the electronic signature) came into effect. (The english translations of the laws have no official character, only German, French and Italian versions are authentic. Therefore the Law and the Ordinance are attached in German version.)

Electronic signatures gain legal status and will carry the same legal weight as handwritten ones.

•recognition of foreign certificates:[960]:
In March 1998, the agreement for reciprocal acceptance of IT-security certificates entered into force (SOGIS-MRA). It was signed by the national authorities of the following states:
Germany, Finland, France, Greece, Great Britain, Italy, Netherlands, Norway, Portugal, Sweden,

[960] cf. Study of the Donau Universität Krems, Master-Studie, Austria

Switzerland and Spain. The agreement was enhanced up to evaluation grade EAL7 on basis of the Common Criteria.

The primary agreement for reciprocal recognition of It security certificates on basis of Common Criteria up to the evaluation grade EAL4 in October 1998 was not signed. The country has not joined the Common Criteria Mutual Recognition Agreement yet.

Availability of Online Services

•eGovernment:

The Swiss Government is keen to promote the use of electronic services, like online voting, and to be among the top countries in the world to use internet and eGovernment services.

•eInvoice:

Annually, about 300 Million invoices are brought into account. Lately, more and more enterprises changed to electronic invoices. To supply authenticity, digital signature is required.[961]

•eVoting[962]

Switzerland started some initiatives to enable electronic voting and started internet test votes in local referenda. Citizens entitled to vote receive all documents via post.

First applications were tested in Genf in January 2003, in Cologny in November 2003, in Carouge in April 2004 and in Meyrin in June 2004. The participation exceeded all expectations.[963]

In November 2004, 8 municipalities voted for the second time over for the Internet in the state of Geneva. No security or technical problems were recorded. The voters received a card including a tamper-proof, a single-use personal ID code as well as an PIN code to allow a secure login to the virtual ballot box. In the participating municipalities, about 22% of the voters voted over the Internet.[964]

Types of electronic signature

The Law defines four different types of signature:[965]

- electronic signature: Data in electronic form, that are attached to other electronic data or are logically linked together and server as authentication.
- advanced electronic signature: is an electronic signature that is exclusively allocated to the signature holder, enabled the identification of the holder, is generated with means that is

---

[961] cf. Tanner, Christian, Wölfle, Ralf, Elektronische Rechnungsstellung zwischen Unternehmen, Fachhochschule beider Basel Nordwestschweiz, Institut für angewandte Betriebsökonomie, 2005

[962] cf. Treasury Board of Canada Secretariat, PKI International Scan - December 2004, http://www.tbs-sct.gc.ca/pki-icp/pki-in-practice/efforts/2004/12/scan-analyse06_e.asp, access on 26.06.2007, 22:02

[963] cf. Arbeitsgruppe E-Voting im BMI, Unterarbeitsgruppe Internationales, Bericht (T.M. Buchsbaum), 20.10.2004

[964] cf. Treasury Board of Canada Secretariat, PKI International Scan - December 2004, http://www.tbs-sct.gc.ca/pki-icp/pki-in-practice/efforts/2004/12/scan-analyse06_e.asp, access on 26.06.2007, 22:02

[965] cf. Study of the Donau University Krems, Master-Study, Switzerland

controlled by the owner and are connected with data they correspond to sot that a later modification of data can be recognized.
- qualified electronic signature: an advanced electronic signature that is based on a secure signature creation device and a qualified and valid certificate.
- signature key: unique data like codes

4.13.2 Application requirements

Types of certificates

In the Law, only qualified and advanced certificates do exist, qualified certificates must be on hardware devices.

•Swisscom provides the following certificates:[966]

- Root CA Certificate
- CA Certificate Class „Diamond“:qualified certificate, for natural persons
- CA Certificate Class „Sapphire“: advanced certificate, for natural and legal persons
- CA Certificate Class „Ruby“: advanced soft-certificate, for natural and legal persons, email, devices, SSL server
- CA Certificate Class Emerald
- TimeStamp CA.

The Certificate Policy and the Certification Practice Statement of SwissCom can be downloaded at http://www.swissdigicert.ch/sdcs/portal/page?node=download_docs&sessionid=955bbc9b7435d3962e110f001df574944cbb186#cp.

•QuoVadis offers the following certificates:[967]

- Qualified Personal Certificate
- Qualified Commercial Certificate
- Advanced Personal Certificate
- Advanced Commercial Certificate
- Commercial EIDI-V Certificate
- Extended Validation SSL Certificate
- SSL, VPN, Domain, Gateway, Code Signing
- Standard Test Certificate

QuoVadis issues mainly Advanced Personal Certificates (about 1000) and qualified certificates are issued in the smallest number (some 100).[968]

---

[966] cf. http://www.swissdigicert.ch/sdcs/portal/page?node=download_ca&sessionid=955bbc9b74f35d3962e110f001df574944cbb186, access on on 16.01.2008, 16:13

[967] cf. http://www.quovadis.ch/page.asp?contentid=22, access on 16.01.2008, 16:04

[968] cf. Correspondence with Carl Rosenast, CEO, QuoVadis Trustlink Schweiz AG, Switzerland

•SwissSign offers certificates for individuals and for devices (figure 116, figure 117).

- Certificates for individuals:

User	Stamping	Label	Carrier	Information
Natural persons	qualified	PostCertificate	hardware (token)	
Natural persons	advanced	PostCertificate	hardware (token)	
Natural persons	advanced	SwissSign	software or hardware ((individual by customer)	
Natural persons with organization entry	advanced	PostCertificate	hardware (token)	
Organizations	conforms to EIDI-V	PostCertificate	hardware (token or HSM)	

Figure 116: Certificates for individuals, issued by SwissSign, source: http://swisssign.com/products-services/certificates-for-natural-and-juridical-persons.html, access on on 16.01.2008, 16:15

- Certificates for Devices:

Certificates for (web) servers
Standard SwissSign Server Certificates
Extended Validation Certificates

Figure 117: Certificates for devices, issued by SwissSign, source: http://swisssign.com/products-services/server-certificates.html, access on on 16.01.2008, 16:15

•Bundesamt für Informatik und Telekommunikation BIT offers the following types of certificates:[969]

- Class A Certificate: Hardware (Token), personal identification, legal signature
- Class B Certificate: Hardware (Token), personal identification, signature, encryption, authentication
- Class C Certificate: Soft-Token, administrative identification, signature, encryption authentication
- Class D Certificate: Soft-Token, administrative identification, authentication
- Code Signing Certificate: Hardware or Software-Token, personal identification, only signature
- Machine Certificate: Soft-Token, administrative identification, mainly authentication

Up to now, BIT has issued 30.000 hardware and 20.000 software certificates, 30.000 advanced and 10 qualified certificates.[970]

The Certificate Policy and Practice Statement can be found on the website at: http://www.bit.admin.ch/adminpki/00240/index.html?lang=de.

[969] cf. http://www.bit.admin.ch/adminpki/00240/index.html?lang=de, access on on 16.01.2008, 16:21

[970] cf. Correspondence with Peter Balsiger, head of the department, Eidgenössisches Finanzdepartment EFD, Bundesamt für Informatik und Telekommunikation BIT, Switzerland

Certification Service Providers

•Swiss OpenLimit Holding AG:

The Swiss Openlimit Holding AG offers solutions for qualified electronic signatures from 40€ upwards. But Openlimit issues only software certificates.[971]

The following certification services provider are accredited in Switzerland:[972]

•Swisscom

SwissCom AG offers a range of services and products:

- "Diamant" Certificate
- Certification Authority (CA)
- Registration Authority (RA)
- LDAP Lightweight Directory Access Protocol (directories)
- Internet Server
- Perimeter defense (Firewall)
- TSA Time Stamping Authorities (Time Stamp Service)
- Card Management

•Quo Vadis Trustlink Schweiz AG

Quo Vadis opens the following range of services and products:

- "Qualified" Certificate
- Certification Authority (CA)
- Registration Authority (RA)
- LDAP Lightweight Directory Access Protocol (directories)
- TSA Time Stamping Authorities (Time Stamp Service)
- Card Management

•SwissSign AG

SwissSign AG offers the following range of services and products:

- "Platinum" Certificate
- Certification Authority (CA)
- Registration Authority (RA)
- LDAP Lightweight Directory Access Protocol (directories)
- Internet Server
- TSA Time Stamping Authorities (Time Stamp Service)
- Card Management

•Die Schweizer Post

---

[971] cf. Correspondence with Ronny Wittig, Openlimit SignCubes AG, Switzerland

[972] cf. Schweizerische Eidgenossenschaft, State Secretariat for Economic Affairs SECO, Public Key Infrastructure, http://www.seco.admin.ch/sas/00229/00251/index.html?lang=en, access on on 16.01.2008, 16:26

•Bundesamt für Informatik und Telekommunikation BIT
BIT offers the following range of services and products:

- "AdminPKI-Class A" Certificate
- (Admin-CA-A-T01)
- Certification Authority (CA)
- Registration Authority (RA)
- LDAP Lightweight Directory Access Protocol (directories)
- Internet Server
- TSA Time Stamping Authorities (Time Stamp Service)

BIT issues all types of certificates.[973]

Table 128 lists up all certification service providers in Switzerland.

Table 128: Certification Service Provider in Switzerland, source: own illustration

Certification Service Provider		Issued Certificates
Openlimit		only software certificates
Swisscom AG		qualified certificates advanced certificates Time stamps
Quo Vadis Trustlink Schweiz AG		qualified certificates advanced qualified certificate SSL Certificate Standard test certificate trusted time stamps
SwissSign AG		qualified certificates advanced certificates time stamps
Bundesamt für Informatik und Telekommunikation BIT		Class A certificates on token Class B certificates on token Class C certificate on soft token Class D certificate on soft token code signing certificate machine certificate

[973] cf. Correspondence with Peter Balsiger, head of the department, Eidgenössisches Finanzdepartment EFD, Bundesamt für Informatik und Telekommunikation BIT, Switzerland

Inspecting authorities[974]

An accreditation is voluntary for certification service provider.

KPMG SA is an independent society that evaluates and judges the conformity of the organization, the infrastructure and the practices of the certification service provider, before it is accredited.

KPMG is currently the only accreditation authority.[975]

4.13.3 Technical preconditions

Signature Software

OpenLimit, the Swiss Holding AG, offers a range of signature solutions. OpenLimits products fulfill essential characteristics: They are certified according to the Common Criteria security standard EAL 4+, support advanced and qualified (secure) electronic signatures in the PDF and PDF/A standard and can be integrated in other applications.[976]

Types of secure signature-creation device

Certificates of the Bundesamt für Informatik und Telekommunikation BIT are available on hardware or soft-token.[977]

Card readers

n.a.

Certificate requirements

n.a.

Application programming interface for online-verification

Certificates of Swisscom can be verified under http://www.swissdigicert.ch/sdcs/certificate/search?node=cert_query&sessionid=541ee9afbc5c1a62457beade3b6d0fbdb38e4319.

Swisscom offers a certification revocation list and also an online certificate status protocol is available.

QuoVadis offers a revocation list on the homepage.

---

[974] cf. Schweizerische Eidgenossenschaft, Federal Office of Communications, Electronic Signature, http://www.bakom.ch/dienstleistungen/faq/01834/01836/index.html?lang=de, access on on 16.01.2008, 16:26

[975] cf. Correspondence with Dr. Klaus Zyla, commercial attaché for Switzerland, Federal Economic Chamber, foreign trade office Zurich

[976] cf. Pressetext, OpenLimit etabliert mit X.Key Vertriebspartnerschaft für Österreich, Press release 21.1.2008, http://www.pressetext.at/pte.mc?pte=080121020, access on

[977] cf. http://www.bit.admin.ch/adminpki/00240/index.html?lang=de, access on on 16.01.2008, 16:26

The Bundesamt für Informatik und Telekommunikation BIT offers a verification service for qualified signatures, an application for advanced signatures is under development.[978]

4.13.4 Summary

Table 129 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 129: Summary and rating, Switzerland, source: own illustration

categories		rating
legal framework	Switzerland was one of the first countries to recognize electronic signatures.	A
technical standard	Swiss Government s keen on promoting the use of electronic services, all types of signature, qualified certificates must be on hardware devices, advanced certificates Hardware and software certificates smartcards, token, 5 accredited CSPs, CRL, OCSP, LDAP	A
distribution	Annually, about 300 million invoices are made, more and more enterprises chance to electronic invoices, requiring digital signatures. no statistics about the actual use of qualified electronic signature. QuoVadis issued about 1.000 advanced personal certificates, qualified certificates are issued in the smallest number (some 100). BIT has issued 30.000 HW and 20.000 SW certificates, 30.000 advanced and 10 qualified certificates.	A

[978] cf. Correspondence with Peter Balsiger, head of the department, Eidgenössisches Finanzdepartment EFD, Bundesamt für Informatik und Telekommunikation BIT, Switzerland

4.14 The Ukraine

Figure 118: Fact-sheet: Ukraine, source: http://europa.eu/abc/european_countries/index_en.htm, access on 21.08.07, 08:56

In figure 118 some basic demographic and geographic data of the country is presented.

4.14.1 Institutional frame

Legislation

In 2003, the parliament approved two laws concerning digital documents and electronic signature. In January 2004, the Law about electronic documents and circulation of e-documents came into effect. This law reflects the conception of the EU directive on electronic signatures (see Appendix – The Ukraine: Law on electronic digital signature).

This law specifies the conditions under which the e-signature has the same status as a handwritten.[979]

But the law presented the requirements for certification of eSignature Centers so complex, that is was impossible for authorities to get accredited. therefore the laws proved generally ineffective up until mid 2005. [980]

Availability of Online Services

•Computer Avaliability:[981]

Computers and software are only for a minority of Ukraine citizens affordable. 48.2% of computers are owned by private, 38.9% of computers by government institutions.

[979] cf. http://www.crime-research.org/library/Belousov_sep.html, access on 17.01.2008, 12:15

[980] cf. Europe‘s Information Society, Political Intelligence Report, Ukraine, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[981] cf. Europe‘s Information Society, Political Intelligence Report, Ukraine, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

•Internet access:[982]

•The use of Internet is growing, but hindered by high cost of internet access and limited computer availability. In August 2006, 10.9% of Ukrainians accessed the Internet. Most of them use Internet for business purposes.

•eCommerce:[983]
eCommerce is under development, because of little Internet penetration and a lack of adequate ePayment systems. Also the legal framework is lacking, but improvements are beeing made.

•eGovernment:[984]
Some initiatives have been taken to develop ICT in government bodies. A government portal[985] was developed which serves as a gateway to sites of different state departments. But as only 12% of authorities have their own website, a lot of work needs to be done.

Types of electronic signature

There are two ways to generate digital signature: hardware and software, provided by Masterkey.[986]

The Government provides electronic signature to sign official documents, but the roll-out of signatures by State Authorities is in an very early stage.[987]

4.14.2 Application requirements

Types of certificates

Masterkey issues qualified public key certificates.[988]

Certification Service Providers

Masterkey Certification Authority is the first authority to be certified in Ukraine.

---

[982] cf. Europe's Information Society, Political Intelligence Report, Ukraine, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[983] cf. Europe's Information Society, Political Intelligence Report, Ukraine, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[984] cf. Europe's Information Society, Political Intelligence Report, Ukraine, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[985] see http://www.kmu.gov.ua/control

[986] cf. source: http://www.masterkey.com.ua, access on 26.07.2007, 00:18

[987] cf. Europe's Information Society, Political Intelligence Report, Ukraine, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[988] cf. http://www.masterkey.com.ua, access on 26.07.2007, 00:18

It is a leading software developer and renders digital signature services for all enterprises, issuing qualified public key certificates.[989]

Table 130 lists up all certification service providers in the Ukraine.

Table 130: Certification Service Provider in the Ukraine, source: own illustration

Certification Service Provider		Issued Certificates
Masterkey CA	MASTERKEY Certification Authority	qualified public key certificates

Inspecting authorities

The certification of eSignature Verification Centers is delegated to SBU, the Security Service of Ukraine.[990]

In 2005, the first „Central National Electronic Digital Signature Certification Body“ was established to carry out accreditation of Certification Centers.[991]

4.14.3 Technical preconditions

Signature Software

Masterkey issues a software for the creation of digital signature, named CA Client Package.[992]

Types of secure signature-creation device

n.a.

Card readers

n.a.

Certificate requirements

n.a.

[989] cf. http://www.masterkey.com.ua, access on 26.07.2007, 00:18

[990] cf. Europe‘s Information Society, Political Intelligence Report, Ukraine, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[991] cf. Europe‘s Information Society, Political Intelligence Report, Ukraine, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45

[992] cf. http://www.masterkey.com.ua, access on 26.07.2007, 00:18

Application programming interface for online-verification

A CRL with all blocked and revoked certificates is published by Masterkey.[993]

4.14.4 Summary

Table 131 sums up the country specifics concerning electronic signature and gives a rating in the areas legal framework, technical standard and market distribution.

Table 131: Summary and rating, The Ukraine, source: own illustration

categories		rating
legal framework	The EU-directive on Electronic Signatures was implemented in 2004. But law proved ineffective as regulations for certification were so complex that no business got accredited. lacking regulations for eCommerce	B
technical standard	eCommerce under development eGov: Initiatives for use of ICT Hardware and software certificates, software for creating digital signatures qualified public key certificates, HW and SW certificates only one CSP, CRL	C
distribution	Few people have access to Internet, thus use of electronic signature service is restricted. eGov and eCommerce under development roll out of signatures in very early stage	C

[993] cf. http://www.masterkey.com.ua, access on 26.07.2007, 00:18

5 Summary

The study surveys the state of practical implementation of infrastructures for digital signatures across Europe. To this end, a total of 21 countries have been analyzed, regarding the legal framework in place, technical standards adopted, and market penetration of signature devices, services, and systems in use.

5.1 Respondents identification

A list of questions was prepared and sent out via e-mail. In total, 661 eMails were sent out. A huge range of e-mail contacts were established and around 22% responses on requests were sent back from different companies and agencies: At the closing of this study, 144 questionnaires have been answered by email correspondence. This is a high number and the survey can be called successfully considering the complexity of the study. The results can be considered as representative, as the answers were sent by specialists about this specialized and technical topic of electronic signatures.

Regarding the geographical locations of the respondents on the email questionnaires, the answers are spread over Europe and beyond: From the 147 responds, 117 answers were sent from the 27 EU member countries, 6 answers from the 3 EU member candidate countries and 24 answers were sent back form the 14 surveyed other European countries (figure 119).

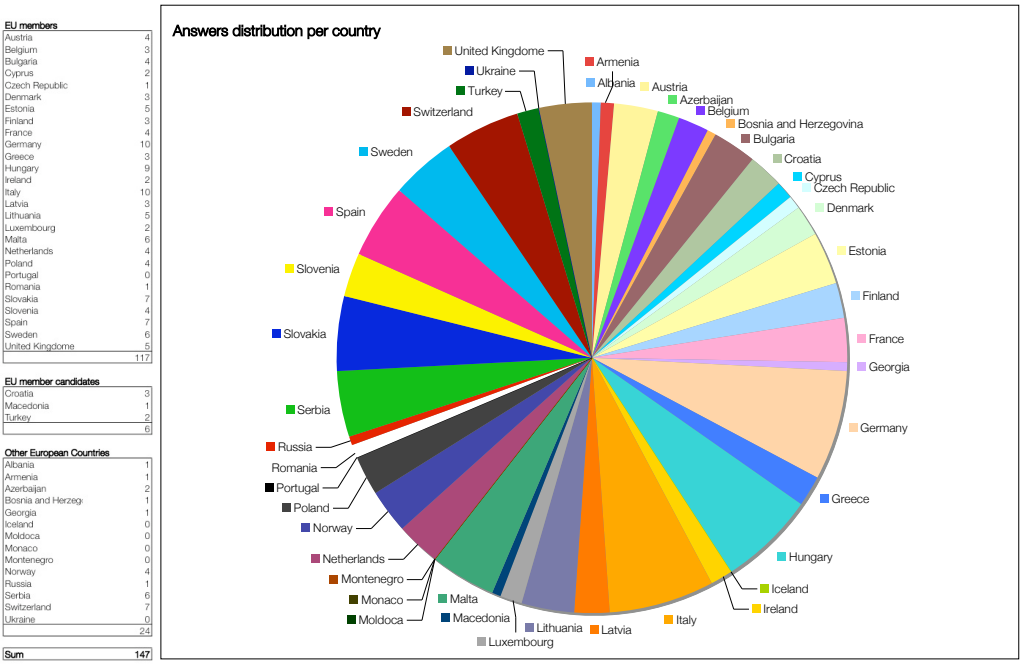


Figure 119: Answers distribution per country, source: own illustration

Some of the sent eMails did not reach the addressee (17%). Reasons are that some stated email contacts are not valid any more or the receiver was out of office (e.g holidays).

5.2 Concluding summary

To gain a general overview, all findings of the study have been centralized in one table. This table shortly presents the status of each country and gives a condensed account of the findings, divided into the three categories used throughout the survey:
(i) institutional frame (IF)
(ii) application requirements (AR)
(iii) technical precondition for electronic signature (TP).

Furthermore, the rightmost column of the tables below shows the assigned 3-letter rating (RT) of each country , repeated from the respective summary table placed at the end of each country analysis chapter.

The color indicates, how much information material has been found for that country.
The letters indice the status of each country: The first position (fist A) stands for the legal framework, the second for the technical standard of electronic signature and the third position denotes the distribution of electronic signature. AAA indicates, that this country has a funded legal framework, high-developed technical standards and a high distribution rate of electronic signatures. CCC notifies that the country is in bad condition, both legally, technically and concerning distribution of electronic signature.
If only less or inadequate information could be found so that no statement concerning the development status or state of use can be given, this will be indicated by the additional character "-".

In tables 133 to 135, abbreviations are used with the following meanings (table 132):

Table 132: key to abbreviation, source: own illustration

abbreviation	stands for	abbreviation	stands for
ADV	advanced electronic signature	OCSP-C	Online Certificate Status Protocol Client
B	basic electronic signature	RS	card reader, connected via Serial port
CRL	Certificate Revocation List	PCCard	PC-Card that serves as card reader
eID	eID card	PCMCIA	PC-Card that serves as card reader
HW	hardware certificate	SC	smartcard
KEYB	card reader, implemented into the keyboard	SIM	SIM card of a mobile phone
L	Lightweight certificate	PIN	PIN-entry
LDAP	Lightweight Directory Access Protocol	SW	software certificate
n.a.	information not available	SSL	SSL certificate
nQ	non-qualified certificate	T	token
no SW	no software certificate exists	USB	card reader that is connected via USB port
OCSP	Online Certificate Status Protocol	Q	qualified certificate

Table 133: summary of all surveyed EU members, source: own illustration

Country	IF		AR			TP					RT
EU members	Law[1]	ES types[2]	C types[3]	CSP[4]	IA[5]	SS[6]	SSCD[7]	CR[8]	R[9]	API[10]	
Austria	1999	B, ADV, Q	Q, nQ	10	2	PDF/A, tust-Desk	eID, eCard	PIN, RS 232, PS/2, USB, KEYB	for citizen Card	CRL	AAB
Belgium	2001	B, ADV, Q	HW, SW, Q, L, SSL	3	1	Aladdin	eID, T SC	USB, RS232, KEYB PCCard, PCMCIA, PIN	for eID card	CRL	AAA
Bulgaria	2001	B,ADV,Q	HW, Q SSL	5	1	OpenSSL, eDocSigner	SC	USB, PCMCIA, PIN	n.a.	CRL	CBB
Cyprus	2004	n.a.	n.a.	n.a.	1	n.a.	n.a.	n.a.	n.a.	n.a.	AC-
Czech Rep.	2001	ADV	HW SW Q	3	1	n.a.	SC	USB, PCMCIA, RS, PIN	for eTax	CRL	AAB
Denmark	2000	ADV	SW, nQ	1	1	n.a.	SC	No sPIN	for OCES	CRL	ACC
Estonia	2002	ADV	HW Q	1	1	n.a.	eID, SIM	PCMCIA, USB, PIN	for eID, DigiDoc	OCSP	BBA
Finland	2003	ADV, Q	HW, SW Q	1	2	n.a.	eID, SC, SIM	USB, PCMCIA, RS, PCCard, KEYB, PIN	for FINEID	CRL	AAA
France	2000	B, ADV, Q	HW, SW, Q	18 (14Q)	1	Applatoo, FAST, AdSigner	eID, SC, T	n.a.	n.a.	CRL OSP	AAA
Germany	1997	B, ADV, Q	HW Q	10	1	n.a.	SC	USB, PCMCIA, RS, PCCard, KEYB, PIN	application component	OCSP, CRL, LDAP	AAB
Greece	2001	B, ADV, Q	HW, SW. B, Q, SSL	7 (3Q)	1	n.a.	SC, T	PCMCIA, USB, KEYB	n.a.	CRL, OCSP	ABA
Hungary	2001	B, ADV, Q	HW, SW, Q	6 (4Q)	3	n.a.	eID, SC, T	n.a.	for eBev, Jelent, DSend	CRL OCSP	BAC
Ireland	2000	B, ADV, Q	B, Q, SSL	2	1	CertifID	n.a.	n.a.	for CertifID	CRL	AA-
Italy	1997. EUdir: 2003	B, ADV, Q	HW, SW, B, Q, L, SSL	18	1	P7m	SC	n.a.	n.a.	n.a.	AAA
Latvia	2002	ADV, Q	HW noSW Q	1	1	eSigner	SC	USB, PCCard, KEYB	n.a.	CRL LDAP OCSP	ABC
Lithuania	2000	B, ADV	HW, SW, Q	1	2	ProSigner, JustaGE	T, SC SIM	USB, PCMCIA, RS, KEYB, PIN	for SC	OCSP	ABB
Lux	2000	B	SSL	1	2		SC, T	USB, PCCard	LuxTrust for SC	n.a.	AC-
Malta	2002	B, ADV	B, nQ	1	1	no	SC	n.a.	n.a.	n.a.	ACC
NL	2003	ADV	HW SSL, Q	4	1	DigiNotar, SafeSign	eID, T SC	USB, PCMCIA, RS PCCard, KEYB, PIN	n.a.	CRL OCSP	AAA
Poland	2001	B, ADV	HW Q, nQ	3	1	n.a.	CitiC SC	RS232, USB PCMCIA	n.a.	CRL OCSP	ABC
Portugal	2003	B, ADV, Q	SW HW SSL, Q	6	n.a.	n.a.	eID, SC	n.a.	n.a.	CRL; OCSP, LDAP	AB-
Romania	2001	B, ADV, Q	SW HW, Q	3	1	FormSeal, DeskSeal	eID, SC, T	n.a.	n.a.	CRL OSCP, LDAP	AAB
Slovakia	2002	ADV, Q	SW,HW Q	15	1	Encrypted mail Explorer,QSign	SC, T	n.a.	n.a.	CRL	BAC
Slovenia	2000	Q	SW HW, Q	5	1	n.a.	SC	n.s.	ActiveX f EPOS	CRL	AAA
Spain	2003	ADV, Q	SW, HW, Q	15	1	n.a.	eID, SC	n.a.	for eID	CRL, OCSP, LDAP	AAA
Sweden	2001	ADV	HW, SW, nQ	10	2	n.a.	eID, SC	n.a.	for eID	CRL OCSP	ABA
UK	2002	B	SW, SSL	4	2	FormPipe	no	no	no	CRL	AC-

Explanation of column headings:

1 Law on electronic signature
2 Types of electronic signature
3 Types of certificates
4 Number of Certification Service Provider
5 Number of Inspecting Authorities
6 Signature Software
7 Types of Secure Signature-Creation Devices
8 Types of Card Readers
9 Certificate Requirements
10 Application Programming Interface for online-verification

Table 134: summary of all surveyed EU member candidates, source: own illustration

Country	IF		AR			TP					RT
EU member candidates	Law[1]	ES types[2]	C types[3]	CSP[4]	IA[5]	SS[6]	SSCD[7]	CR[8]	R[9]	API[10]	
Croatia	2002	B, ADV	HW, SW, Q, SSL	1	1	yes	SC	USB, RS, PIN	Yes	CRL	ABC
Rep. of Macedonia	2001	n.a.	SW, B, Q, SSL	1	n.a.	n.a	T	n.a.	n.a.	n.a	BC-
Turkey	2004	ADV	SW, HW, Q	4	1	n.a.	SC, T	n.a.	n.a.	CRL OCSP	ABB

Table 135: summary of all surveyed European countries, source: own illustration

Country	IF		AR			TP					RT
other Europ. countries	Law[1]	ES types[2]	C types[3]	CSP[4]	IA[5]	SS[6]	SSCD[7]	CR[8]	R[9]	API[10]	
Albania	n.a.	no	no	no	no	no	no	no	no	no	-CC
Armenia	2002	n.a.	SW, SSL	1	1		n.a.	n.a.	n.a.	CRL	BCC
Azerbaijan	2002	n.a.	n.a.	n.a.	1	n.a.	n.a.	n.a.	n.a.	n.a.	AC-
Bosnia and H.	2006	n.a.	n.a.	no	n.a.	n.a	n.a.	n.a.	n.a.	n.a.	ACC
Georgia	2000	n.a.	n.a.	1	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	ACC
Iceland	2001	B	n.a.	1	1	n.a.	eID, SC	n.a.	n.a.	n.a.	AC-
Moldova	2004	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a	n.a.	n.a.	ACC
Monaco	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	---
Montenegro	2003	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	ACC
Norway	2001	n.a.	n.a.	n.a.	1	n.a.	eID, SC	n.a.	n.a.	n.a	AB-
Russia	2002	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	ACC
Serbia	plan08	B, ADV, Q	HW, SW, Q, SSL	1	1	n.a.	SC, T	USB, no PIN	yes	CRL	CBC
Switzerland	2005	ADV, Q	HW, SW, Q SSL	5	1	yes	SC T	n.a.	n.a.	CRL, OCSP, LDAP	AAA
The Ukraine	2003	n.a.	HW, SW QPKI	1	1	CA Client	n.a.	n.a.	n.a.	CRL	BCC

Explanation of column headings:

1 Law on electronic signature
2 Types of electronic signature
3 Types of certificates
4 Number of Certification Service Provider
5 Number of Inspecting Authorities
6 Signature Software
7 Types of Secure Signature-Creation Devices
8 Types of Card Readers
9 Certificate Requirements
10 Application Programming Interface for online-verification

On closer inspection of the last tables, a lot of dynamics can be noticed.

The European Commission implemented a community framework for electronic signatures, European Directive 1999/93/EC. The main objective was to create a framework for the use of electronic signatures, to allow a free cross border flow of signature products and services and to ensure a basic legal

recognition.[994]
In EU member states, strong endeavors have been undertaken to implement a legal framework for electronic documents and digital signatures and to develop markets for such applications, mainly in the years 2000-2001. Since then, comparatively few follow-up measures have been taken, giving the impression that the "high time" of electronic signature has already passed by within the European Union. Thus, also for the years to come little activity is to be expected indeed.

By contrast, the remaining countries surveyed are not at the same level of development yet. Although the legal framework has been set up in nearly every country, legal regulation and technical implementation strike a kind of balance. In some countries, in fact, a nearly unmanageable diversity of technical standards and applications is observable.

The present study demonstrates quite clearly that no wide-area implementation of digital signatures has been achieved yet, mostly because of lacking technical interoperability of systems, processes and configurations, while the uniform legal framework is certainly not the barrier. It is not very hard to understand that the benefits of a broad adoption of digital signature in the European economic area cannot be realized this way.

In most countries, qualified electronic signatures have the same legal value as handwritten signatures. But in some countries, electronic signatures are only partly regulated (e.g., Estonia, Slovakia), or electronic signatures are not recognized at all, like in Bulgaria. National laws constitute different requirement for recognition of signatures. By adopting the European Directive to national laws, the European legislator determines a type of signature that will consequently be considered as equivalent to handwritten signature in every Member State.

From the technical perspective, the European Directive has influenced and evoked a lot of international initiatives for standardization and harmonization as well as a lot of activities concerning the development and enhancement of online services, eGovernment and applications for electronic signatures.[995]

The World Market Research Center examined eGovernment applications of 196 countries worldwide. Criteria for the evaluation include: availability of online information, access feasibility for citizens, access over a single portal, online-payment, access for handicapped persons and value performance. European countries did not hit the spot in this survey, on average, Europe reached 34,1 % of the points, as european websites don‘t provide a lot of relevant functions. The ranking of the study of 2001 can be found in the Appendix - Miscellaneous: Global E-Government Survey 2001, Ranking.
Data protection and security are of great concerns but many government websites miss to inform citizen about data protection and safety regulations. Uncertainty about the security of an online transaction blocks the acceptance of eGovernment services. Also the lack of usability for handicapped people, misses the mark of eGovernment initiatives to achieve a great number of users.

---

[994] cf. Commission of the European Communities, Report from the commission to the European Parliament and the Council, Brussels, 15.3.2006

[995] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

The lacking possibility to pay with credit cards or use electronic signatures constrains an overall exercise of online services. The whole study can be found on http://www.wmrc.com.[996]

A lot of countries have started electronic identity card initiatives and developed eID cards, storing electronic certificates for authentication and digital signing.
EU member states like Belgium, Italy, Finland, Estonia or Spain have issued eID cards that store qualified certificates. Others are planning to launch dID cards, like Portugal that plans to make an eID card available by 2008[997] or Germany, that pans to issue eID cards starting in 2008.[998]

But the adoption of eSignature applications has also entailed some difficulties.
One big obstacle to the acceptance and proliferation of electronic signatures is the lack of interoperability of systems and applications, both national and cross border. For example, many applications only accept certificates form one certification authority.
Another problem is the lack of transparency that has created confusion in the market [999], like of existing signatures standards or legal requirements.

The different countries seek to reach a high level of interoperability and legal recognition of electronic signatures within and beyond Europe.[1000]

To further the use of electronic signatures, the European Commission and a range of private have started initiatives. The European Commission considers the promotion of electronic services and applications as necessary and to regard the technological development. Moreover, the Commission will also encourage further standardization work to assist a nationwide and cross-national interoperability of eSignature systems and the use of all types of technologies for qualified electronic signatures.[1001]

Due to an increasing diffusion of electronic identity cards and the adoption of electronic signatures in electronic administration services, like eTaxing services, it is assumed that the demand for electronic signature will aggravate and the European Directive 1999 will serve as solid base for the use and insertion of electronic signature.[1002]

---

[996] cf. World Market Reseach Centre, Europa hinkt beim E-Government Nordamerika hinterher, News Release, 18.10.2001, http://www.prnewswire.co.uk/cgi/news/release?id=75335, access on 27.06.2007, 13:00

[997] cf. European Commission, eGovernment Factsheet, eGovernment in Portugal, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08

[998] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[999] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[1000] cf. Dumortier, Jos, Kelm, Stefan, et al., The legal and market aspects of electronic signatures, Study for the European Commission, 2004

[1001] cf. European Commission, Kommissionsbericht: Elektronische Signaturen werden trotz rechtlicher Anerkennung noch kaum grenzübergreifend verwendet., Press release, 17.03.2006, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/325&format=HTML&aged=0&language=DE&guiLanguage=en, access on 4.12.2007

[1002] cf. European Commission, Kommissionsbericht: Elektronische Signaturen werden trotz rechtlicher Anerkennung noch kaum grenzübergreifend verwendet., Press release, 17.03.2006, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/325&format=HTML&aged=0&language=DE&guiLanguage=en, access on 4.12.2007

In addition, the European Commission and other institutions must promote the use of eSignature and encourage the private and public sector to take advantage of electronic services.
Still, however, it is hoped that this study contributes significantly to the promotion of the very idea by charting the current digital signature landscape of Europe.

Glossary

Advanced Electronic Signature

An advanced electronic signature is an electronic signature that

a) is uniquely linked to a signatory,
b) is capable of identifying the signatory,
c) is created using means that are under the signatory's sole control, and
d) is linked to other electronic data in such a way that any alteration to the said data can be detected.[1003]

Card Reader

A peripheral device that reads the magnetic stripe on the back of a credit card.[1004]

Certificate

A certificate is an electronic statement, mapping the signature verification data to confirm the identity of the person.[1005]

Certification Authority (CA)

An organization that issues digital certificates is called Certification Authority.[1006]

Certification Policy (CP)

A certification policy is part of the certification concept, in which regulations for the issuance of certificates are published.[1007]

[1003] cf. Qualified Electronic Signatures Act (SFS 2000:832), Sweden

[1004] cf. http://www.pcmag.com/encyclopedia

[1005] cf. FedCT, Belgium Root CA – Certification Practice Statement, 2003

[1006] cf. FedCT, Belgium Root CA – Certification Practice Statement, 2003

[1007] cf. Rundfunk und Telekom Regulierungs GmbH, 4 Jahre Signaturgesetz, Schriftreihe, Band 1/2004

Certification Practive Statement (CPS)

The Certification Practice Statement is part of the certification concept, in which a certification service provider formulates how it procedes when issuing certificates.[1008]

Certification Service Provider (CSP)

The legal or natural person who issues certificates or who guarantees that the certificate of others complies with certain requirements.[1009]

Certificate Revocation List (CRL)

The certification authority provides a list that includes revoked and suspended certificates. This list is digitally signed by the CA and can bee consulted by relying parties before trusting information featured in certificates.[1010]

Digital Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.[1011]

Digital Signature

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.1012
A digital signature is a subset of electronic signature.

In contrast to an electronic signature, a digital signature itself is a unique numerical value based on the entire written document that is being signed.[1013]

[1008] cf. Rundfunk und Telekom Regulierungs GmbH, 4 Jahre Signaturgesetz, Schriftreihe, Band 1/2004

[1009] cf. Qualified Electronic Signatures Act (SFS 2000:832), Sweden

[1010] cf. FedCT, Belgium Root CA – Certification Practice Statement, 2003

[1011] cf. http://www.searchsecurity.com

[1012] cf. http://www.searchsecurity.com

[1013] cf. http://www.out-law.com

eGovernment

It is a synonym for a modern and efficient administration. It is the insertion of Information and Communication Technology in the public administration to improve public services and democratic processes and ease the configuration and execution of governmental politics.[1014]

eID

The eID is the system of the e-ID card, including the organisation, infrastructure, all procedures, contracts and necessary resources, related to the eID card.[1015]

Electronic Signature

In contrast to a digital signature, an electronic signature can include a printed name, an e-mail address, and a scanned signature.[1016]

LDAP

(Lightweight Directory Access Protocol) A protocol used to access a directory listing.[1017]

is an Internet standard for common (simple) directories, representing a global model of directory services and being based on the TCP/IP protocol. It is defined in the IETF RFC 1777 “The Lightweight Directory Access Protocol” standard.[1018]

OCSP

OCSP (Online Certificate Status Protocol) is one of two common schemes for maintaining the security of a server and other network resources. The other, older method, which OCSP has superseded in some scenarios, is known as Certificate Revocation List.[1019]

PIN

is a series of symbols used for identifying the holder of the identification means.[1020]

[1014] cf. http://www.digitales.oesterreich.gv.at

[1015] cf. FedCT, Belgium Root CA – Certification Practice Statement, 2003

[1016] cf. http://www.out-law.com

[1017] cf. http://www.pcmag.com/encyclopedia

[1018] cf. Ordinance on the Activities of Certification-Service-Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services

[1019] cf. http://www.searchsecurity.com

[1020] cf. Ordinance on the Activities of Certification-Service-Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services

Private Key

The private key is a mathematical key that creates digital signature and to decrypt documents and data when combining with the corresponding public key.[1021]

Public Key

The public key is a mathematical key, used to verify signatures that have been created with the corresponding private key. The public key can also be used to encrypt data, which can then be decrypted only with the corresponding private key.[1022]

Public Key Infrastructure (PKI)

PKI is an acronym and describes the system of the Public Key cryptography that is combined with an Infrastructure, which enables to provide a security level for communicating and storing electronic information.1023 It is a system that integrates software, encrypting technology and other services, that enables secure business transactions and data transmission of e-documents.[1024]

The PKI should create trust in electronic information by governments, business and consumers.[1025]

It is a system that integrates software, encrypting technology and other services, that enables secure business transactions and data transmission of e-documents.

Qualified Certificate

The public key is a mathematical key, used to verify signatures that have been created with the corresponding private key. The public key can also be used to encrypt data, which can then be decrypted only with the corresponding private key.1026

Qualified Electronic Signature

Is an advanced electronic signature based on a qualified certificate and created by a secure signature creation device.[1027]

[1021] cf. FedCT, Belgium Root CA – Certification Practice Statement, 2003

[1022] cf. FedCT, Belgium Root CA – Certification Practice Statement, 2003

[1023] cf. FedCT, Belgium Root CA – Certification Practice Statement, 2003

[1024] cf. National Association of Local Authorities in Denmark et al, Nikolova, Maria, The E-Era and Bulgarian administration, Public Management Forum, A Review for Public Administration Practitioners in Centras and Eastern Europe and the CIS, Vol. VII, No. 2-3 December 2002

[1025] cf. FedCT, Belgium Root CA – Certification Practice Statement, 2003

[1026] cf. FedCT, Belgium Root CA – Certification Practice Statement, 2003

[1027] cf. Qualified Electronic Signatures Act (SFS 2000:832), Sweden

Secure Signature-Creation Device

A signature creation device is a software or hardware used to implement the signature creation data.[1028]

It satisfies the legal requirements of a signature in relation to data in electronic form in the same manner as a hand written signature.

xAdES

XML based advanced electronic signature

It provides basic authentication and integrity protection and can be created without accessing on-line (time-stamping) services. However, without the addition of a time-stamp or a secure time record the electronic signature does not protect against the threat that the signer later denies having created the electronic signature.[1029]

X.509 Standard

This Standard concerns the coding of certificates and revocation lists.[1030]

[1028] cf. Qualified Electronic Signatures Act (SFS 2000:832), Sweden

[1029] cf. http://www.w3.org/TR/2003/Note-Xades-20030220

[1030] cf. Rundfunk und Telekom Regulierungs GmbH, 4 Jahre Signaturgesetz, Schriftreihe, Band 1/2004

Bibliography

Literature

Andersson, H., Bylund, M., Olsson, A. R., Olsson, O., Seipel, P. & Sjödin, G., *Survey of Privacy and Information Technology*, SAITS project, Technical Report V.1.0, 2003

Arbeitsgruppe eVoting im BMI, Unterarbeitsgruppe Internationales, Bericht (T.M. Buchsbaum), 20.10.2004

Babovic, Zoran, Darko, Jovic, Milutinovic, Velijko, Survey of eGovernment Services in Serbia, *Informativa* 31 (2007) 379-396, 26.August 2007

Certification Europe Ltd., *Qualified Electronic Signatures and Certification*, Support of Certification Europe's Certification Scheme, Fact Sheet June 2003

Commission of the European Communities, Communication form the Commission to the council, the European Parliament, the European economic and social committee and the committee of he regions, *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*, 25.04.2006, Brussels

Day, Ruth, *Comments on Draft „Electronic Signature Law" of the Azerbaijan Republic*, February 2002

Deborah Asbrand, *E-Government: Kleine Länder groß im Internet*, press release, Heise.de, Technology Review, 7.10.2004

Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. & Van Eecke, P., *The legal and market aspects of electronic signatures*, Study for the European Commission, 2004

Dumortier, J., *Legal Status of Qualified Electronic Signatures in Europe*, in ISSE 2004-Securing Electronic Business Processes, 2004

Economist Intelligence Unit, Russia: Overview of e-commerce, Article in *Global Technology Forum*, 05.December 2006

European Commission, IDABC, *Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications*, April 2007

Evolaris Solution Center, *Akzeptanz elektronischer Signatur*, Wissenschaftlicher Bericht im Auftrag des BMWA, Dezember 2003

FedCT, Belgium Root CA - *Certification Practice Statement*, 2003

FedCT, *EID Hierarchie and Certificate Profiles*, Ref: EID-DEL-004 - V3.1, February 2006

Gerstbacher, Peter, *Die österreichische Bürgerkarte*, Bakkalaureatsarbeit, Studiengang Wirtschaftinformatik, TU Wien, 2005

Government of Romania, Ministry of Public Administration – the Government's strategy concerning the National Action Plan, *e-Administration*, Bucharest – 2001

Hauber, Julia, *Faktische Probleme der elektronischen Signatur*, Seminararbeit, WU Wien, 2003

Höpner, Petra, *Study PKI and Certificate Usage in Europe 2006*, Fraunhofer Institute FOKUS, 2006

Jaak Tepandi, Arvo Ott, *eSecurity activities 2004*, Presentation, SOIS meeting, 01.10.2004

Menais, Alexandre, *Electronic Signatures in France*, July 2002

National Association of Local Authorities in Denmark et al, *Digital Administration*, Mai 2001

Naumov, Victor, Nikiforva, Tatiana, Electronic signatures in Russian Law, *The e-Signature Law Journal*, December 2005

Nielsen, Jeannette, Meinertz, Ulrik, *Denmark Launches Nationwide Digital Signatures*, March 2003

Nikolova, Maria, The E-Era and Bulgarian administration, Public Management Forum, *A Review for Public Administration Practitioners in Centras and Eastern Europe and the CIS*, Vol. VII, No. 2-3 December 2002

Nuster, Michael, *Spezifische Fragen im Zusammenhang mit elektronischen Signaturen*, 2005

Panayiotou, Panayiotis Andrea, *Electronic Governance for the Lands and Surveys Department in Cyprus*, FIG Working Week 2004, AThens, Greece, May 22-17, 2004

Rundfunk und Telekom Regulierungs GmbH, *4 Jahre Signaturgesetz*, Schriftreihe, Band 1/2004

Sealed, DLA Piper and Across communications, *Study on the standardisation aspects of eSignature*, final report, 22.11.2007

Spassov, Kamen Boyanov, Seaul, *Application of the Digital Opportunity Index to Bulgaria*, Sept 1, 2006

Tanner, Christian, Wölfle, Ralf, *Elektronische Rechnungsstellung zwischen Unternehmen,* Fachhochschule beider Basel Nordwestschweiz, Institut für angewandte Betriebsökonomie, 2005

Treasury Board of Canada Secretariat, *PKI International Scan*, December 2004

UNDP Moldova, *Advancing e-Government Solutions for Friendly, Efficient and Secure Public Services*, press release, UNDP, April 2007

UNDP, United Nations Development Programme and the Government of Bosnia and Herzegovina, *Development of HiH ICT Strategy*, Preparatory Assistance Document, 1.7.2003

Online sources

A-Cert		http://www.a-cert.at	http://www.a-cert.at/php/cms_monitor.php?q=FAQ-A-CERT, access on 28.11.2007, 18:38
A-Trust		http://www.a-trust.at	http://www.a-trust.at/default.asp?lang=GE&ch=3&node=550, access on 06.11.2007, 17:25 Transaktionssicherheit Sicherer Signaturen, V. 1.0, April 2006 http://www.a-trust.at/docs/Transaktionssicherheit_Sicherer_Signaturen.pdf access on 06.11.2007, 18:02
A1 Austria		http://www.a1.net	http://www.a1.net/business/a1signaturablauf, access on 9.11.2007, 15:24
Actalis		http://www.actalis.it	http://www.actalis.it/en, access on 03.12.2007, 18:54
ADACOM		http://www.adacom.com	http://einvoices.idealsystems.gr/Adacom/Products_Services/PKI%20%20Authentication/Case%20Studies/ E_Sign.aspx, access on 09.08.07, 09:18 http://www.adacom.com/index.php?option=com_content&task=category&sectionid=7&id=29&Itemid=91, access on 09.08.2007, 09:19
AET Europe		http://www.aeteurope.nl	http://www.aeteurope.nl/SafeSign/SafeSign_Identity_Client_Specifications, access on 25.08.07, 23:24
American University Washington D.C.		http://www.american.edu	IT Landscape in Armenia http://www.american.edu/carmel/hs9920a/armenia/encryption_in_armenia.htm, access on 27.12.2007, 09:02
Arbeitsgemeinschaft für witschaftliche Verwaltung e.V.		http://www.awv-net.de	http://www.awv-net.de/cms/font_content.php?idcat=23&prod_id=68 , access on 09.08.2007, 09:24

ARDACO		http://www.ardaco.com	http://www.ardaco.com, access on 27.06.07, 12:19
B-Trust		http://www.b-trust.org	http://www.b-trust.org, access on 18.07.07, 19:34
Bull		http://www.bull.com	http://www.bull.com/bulldirect/N8/rybnik.html, access on 27.06.2007, 10:25
Bund des Inneren, KBSt		http://www.kbst.bund.de	http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/Initiativen/Bol/bol.html__nnn=true http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/egov__inhalt.html, access on 6.11.2007, 17:59 http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/Initiativen/EGov2/EGov2.html__nnn=true, access on 6.11.2007, 17:56
Bundesamt für Informatik und Telekommunication BIT		http://www.bit.admin.ch	http://www.bit.admin.ch/adminpki/00240/index.html?lang=de, access on on 16.01.2008, 16:21
Business Line		http://business-line.com	http://business-line.com/business-weekly/archieves/362/04.htm, access on 27.06.2007, 12:23
Cardreaders.be		http://www.cardreaders.be/	http://www.cardreaders.be/en/default.htm, access on 18.07.2007, 11:12
Certification Europe		http://www.certificationeurope.com	http://www.certificationeurope.com/company/default.asp, access on 28.07.07, 19:54
Certipost		http://www.e-trust.be	http://www.e-trust.be/, access on 13.07.2007, 16:07
CertPlus/ Keynectis		http://www.certplus.com http://www.keynectis.com/	http://www.certplus.com/, access on 13.11.2007, 11:37 http://www.keynectis.com/en/index.html, access on 14.11.2007, 19:37

Challenge Liberty and Security		http://www.libertysecurity.org	http://www.libertysecurity.org/article520.html, access on 04.08.07, 16:55 http://www.libertysecurity.org/article511.html, access on 01.08.2007, 23:59
Computer Crime Research Centre		http://www.crime-research.org	http://www.crime-research.org/library/Belousov_sep.html, access on 17.01.2008, 12:15
Data State Inspection	DATU VALSTS INSPEKCIJA	http://www.dvi.gov.lv/eng	http://www.dvi.gov.lv/eng, access on 30.07.07, 16:16
DataProtection.eu	dataprotection.eu	http://www.dataprotection.eu	http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.AL, access on 27.06.2007, 12:43
DigiD	DigiD	http:/www.digid.nl/english	http:/www.digid.nl/english, access on 04.08.07, 16:11
DigiNotar Internet Trust Service	DigiNotar Internet Trust Services	http://www.diginotar.com	http://www.diginotar.com/Default.aspx?tabid=95, access on 04.08.07, 20:39 http://www.diginotar.com, access on 04.08.07, 19:50
Digitales Österreich	DIGITALES ÖSTERREICH	http://www.digitales.oesterreich.gv.at	Digitales Österreich, Was ist E-Government?, http://www.digitales.oesterreich.gv.at/site/5230/default.aspx, access on 01.10.2007, 11:16
Digital Media News for Europe	DMeurope.com Digital media news for europe	http://www.dmeurope.com	http://www.dmeurope.com, access on 26.06.2007, 18:12 http://www.dmeurope.com/default.asp?ArticleID=6086, access on 26.06.2007, 18:10 http://www.dmeurope.com/default.asp?ArticleID=6086, access on 26.06.2007, 18:10
E-Guvernare	e-guvernare sistemul electronic national	http://www.e-guvernare.ro	http://www.e-guvernare.ro/default.aspx?LangID=4, access on 09.08.07, 07:19 http://ac.e-guvernare.ro/pc/, access on 05.12.2007, 20:10

E-Lock		http://www.elock.com	http://www.elock.com/bank-romania.html, access on 25.07.2007, 18:29 http://www.elock.com, access on 25.07.2007, 18:29 E-Lock, XML Signing Solution, http://www.elock.com/ xml-signing.html, access on 1.10.2007, 12:23 http://www.elock.com, access on 26.06.2007, 19:29
e-Signature Law Journal		http://www.e-signaturelawjournal.co.uk http://deaeslr.org	Naumov, Victor, Nikiforova, Tatiana, Electronic signatures in Russian law, The e-Signature Law Journal, December 2005, http://www.e-signaturelawjournal.co.uk, access on 10.01.2008, 10:40
ECIN		http://www.ecin.de	ECIN, Digitale Rechnungen: aber sicher!, press release, 10.5.2005, http://www.ecin.de/news/2006/05/10/09472/index.html, access on 14.11.2007, 19:05
eCroatia		http://www.e-hrvatska.hr	http://www.e-hrvatska.hr/sdu/en/ProgramEHrvatska/OPrograma.html, access on 01. 08.2007, 19:21
eDocuments		http://einvoices.idealsystems.gr	http://einvoices.idealsystems.gr/Adacom/Products_Services/PKI%20%20Authentication/Case%20Studies/ E_Sign.aspx, access on 09.08.07, 09:18
eGov Project Macedonia		http://e-gov.org.mk	http://www.e-gov.org.mk/about.htm, access on 01.08.07, 10:19 http://www.e-gov.org.mk/tender_q&a_summaray.htm, access on 01.08.07, 10:21
eGovernment Resource Centre		http://www.egov.vic.gov.au	eGovernment - Netherlands – Archive, http://www.egov.vic.gov.au/index.php?env=-innews/detail:m1184-1-1-8-s-0:n-146-1-0--, access on 04.08.07, 21:12

eHealth Platform doctor.am	http://www.doctor.am	http://www.doctor.am, access on 4.12.2007, 17:12
eHealth Portal Azerbaijan doctor.az	http://doctor.aznet.org	http://doctor.aznet.org, access on 4.12.2007, 17:13
eID services	http://repository.eid.belgium.be	http://repository.eid.belgium.be , access on 08.08.07, 13:24
eLuxembourg	http://www.eluxembourg.public.lu	http://www.eluxembourg.public.lu, access on 14.11.2007, 19:09
ePractice.eu	http://www.epractice.eu	European Commission, eGovernment Fact-sheet - Slovenia - National Infrastructure, 14.December 2007, http://www.epractice.eu/document/3474, access on 04.12.2007, 17:08 http://www.epractice.eu/index.php?page=document&doc_id=3404&doclng=6, access on 15.06.2007, 19:36 European Communities, EU: i2010 is starting to deliver, http://www.epractive.eu/document/4644, access on 2.10.2007, 09:33 ePractice.eu, eGovernment Factsheet - Greece - National Infrastructure, 14 December 2007, http://www.epractice.eu/document/3368, access on 10.1.2007, 09:12 http://www.epractice.eu/index.php?page=document.print&type=&doc_id=3323&doclng=6, access on 25.08.07, 01:18
EquifaxSecure	http://www.equifaxsecure.co.uk	http://www.equifaxsecure.co.uk/policies/crlcheck.html, access on 27.07.07, 14:12 http://www.equifaxsecure.co.uk/digitalcertificates/dc_webservcert.html, access on 27.06.07, 14:14

Estonian Informatics Centre 	http://www.ria.ee http://www.riso.ee	http://www.ria.ee, access on 21.07.2007, 21:56
European Commission, IDABC	http://ec.europa.eu/idabc	Europe's Information Society, Political Intelligence Reports, http://ec.europa.eu/information_society/activities/internationalrel/index_en.htm, access on 28.12.2007, 18:45 European Commission, eGovernment Factsheet, March 2007, http://ec.europa.eu/egov, access 04.12.2007, 17:08 European Commission, eProcurement, http://ec.europa.eu/idabc/en/document/2084/5874, access on 1.10.2007, 9:12 European Commission, IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profiles, April 2007, http://ec.europa.eu/idabc/en/chapter/6000, access on 28.11.2007, 13:24 European Commission, IDABC, The Programme, http://ec.europa.eu/idabc/en/chapter/3, access on 28.11.2007, 13:24 European Commission, IDABC, Token Type, http://ec.europa.eu/idabc/en/chapter/6004, access on 23.11.2007, 13:32 European Commission, Information Society, eTEN Brochure, http://ec.europa.eu/information_society/activities/eten/index_en.htm, access on 1.10.2007, 9:14 European Commission, http://ec.europa.eu, access on 15.06.07, 20:00

			European Commission, http://ec.europa.eu/idabc/en/document/3697/590, access on 26.06.07, 18:08 European Commission, http://ec.europa.eu/idabc/en/document/5923, access on 15.06.2007, 18:09 European Commission, http://ec.europa.eu/idabc/en/document/6129/411, access on 27.06.07, 12:07 European Commission, http://ec.europa.eu/idabc/en/document/6574/194, access on 26.06.07, 17:39 European Commission, http://ec.europa.eu/idabc/servlets/Doc?id=29084, access on 01.08.2007, 19:43 European Commission, http://ec.europa.eu/information_society/activities/egovernment_research/countries/norway/ European Commission, http://ec.europa.eu/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm#malta, access on 26.06.2007, 23:12
eVO eTendering Portal		http://www.evo.gov.sk	http://www.evo.gov.sk, access on 28.11.2007, 13:39
Finish Data Ombudsmann		http://www.tietosuoja.fi	http://www.tietosuoja.fi/1560.htm, access on 25.07.2007, 12:02
Finnish Population Register Centre		http://www.vaestorekisterikeskus.fi http://www.fineid.fi/en	http://www.fineid.fi/en, access on 18.08.2007, 12:32 http://www.fineid.fi/vrk/fineid/home.nsf/pages/105C03AFB213C30EC2257054002DB6E2, access on 25.07.2007, 09:49

			http://www.fineid.fi/vrk/fineid/home.nsf/pages/C3B39DB2DB61D6B7C2257054002DB718, access on 25.07.2007, 09:17 http://www.vaestorekisterikeskus.fi/crk/home.nsf/www/electronic identity, access on 25.07.2007, 9:10 http://www.vaestorekisterikeskus.fi/vrk/fineid/files.nsf/files/AB5241964425FBF1C22572ED001B9EDC/$file/4_Summary+of+the+country+updates.pdf, access on 21.08.2007, 23:24 http://www.vaestorekisterikeskus.fi/vrk/fineid/home.nsf/pages/11536F2A8FC6C794C2257054002DEC65, access on 24.07.2007, 09:48 http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/9C0B5FFC32EC6AF2C2257244005112 98?opendocument, access on 25.07.2007, 9:12 http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/A0D3A8D03E6882C5C22572440052 13EC?opendocument, access on 25.07.2007, 9:13 http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/FE039B4246B8FED9C22572450036E7E6?opendocument, access on 25.07.2007, 09:16 http://www.vaestorekisterikeskus.fi/vrk/home.nsf/www/about, access on 25.07.2007, 9:10 www.vaestorekisterikeskus.fi/.../4036B970E0CAA61BC2257219004E5639/file/Summary_of_the_country_updates.doc, access on 21.08.2007, 23:29
Gazeta Start	gazeta start www.gazetastart.com	http://gazetastart.com/	http://gazetastart.com/?faqe=shfaqflash&LajmID=18076, published on 05.01.2008, 16:38, access on 16.01.2008, 11:42
GBO.Overheid	GBO.OVERHEID	http://gbo.overheid.nl/english	http://gbo.overheid.nl/english, access on 04.08.07, 16:14
Gemalto	gemalto security to be free	http://www.gemalto.com	http://www.gemalto.com, access on 25.08.2007, 08:25
Geonetric's Pink-Roccade	Getronics PinkRoccade	http://www.pinkroccade.nl	http://www.pinkroccade.nl, access on 04.08.07, 21:23
GIE Sesam Vitale	sesam-vitale	http://www.sesam-vitale.fr	GIE sesam viatale, the SESAM-Vitale program, http://www.sesam-vitale.fr/programme/programme_eng.asp, access on 14.11.2007, 19:46

Global Technology Forum		http://globaltechforum.eiu.com	http://globaltechforum.eiu.com/index.asp?layout=rich_story&channelid=4&categoryid=31&title=Turkey%3A+Overview+of+e-commerce&doc_id=11173, access on 01.08.2007, 23:48 Economist Intelligence Unit, Russia: Overview of e-commerce, 05.December 2006, Article in Global Technology Forum, http://globaltechforum.eiu.com/index.asp?layout=rich_story&doc_i…title=Russia%3A+Overview+of+e-commerce&channelid=4&categoryid=29, access on 10.01.2008, 10:25
Government of Malta		http://www.gov.mt	http://www.gov.mt/egovernment.asp?p=105&l=1, access on 26.06.2007, 22:02
Halcom CA		http://www.halcom-ca.si	Halcom CA, Identity of certificate authority Halcom CA, http://wwweng.halcom-ca.si/index.php?section=14, access on 10.12.2007: 13:27 http://wwweng.halcom-ca.si/, access on 10.12.2007, 19:32 http://wwweng.halcom-ca.si/index.php?section=18, access on 28.11.2007:13:13
Heise Online		http://www.heise.de	Heise Online, Feinschliff für OpenOffice, press release, 27.3.2008, http://www.heise.de/newsticker/Feinschliff-fuer-OpenOffice--/meldung/105557, access on 27.03.2008, 15:38
Help.gv Portal		http://www.help.gv.at	http://www.help.gv.at, access on 4.12.2007, 18:41
ID card		http://www.id.ee	http://www.id.ee access on 21.07.2007, 12:12
Ilex France		http://www.ilex.fr	http://www.ilex.fr/en/produits/applatoo-presentation.htm, access on 14.11.2007, 19:51
InfoNotary		http://www.infonotary.com	http://www.infonotary.com, access on 19.07.07, 11:12

Information System Security special purpose server		http://www.ssi.gouv.fr	http://www.ssi.gouv.fr/fr/index.html, access on 14.11.2007, 19:56
Internet4jurists		http://www.internet4jurists.at	http://www.internet4jurists.at, access on 10.06.2007, 13:51
IT Solution		http://www.itsolution.at	IT solutions, Produkte, http://www.itsolution.at/DE/produkte.html, access on 07.11.2007, 15:18
IT Wissen		http://www.itwissen.info	IT Wissen, eGovernment, http://www.itwissen.info/definition/lexikon, access on 1.10.2007, 11:14
Kamu		http://www.kamusm.gov.tr/en	http://www.kamusm.gov.tr/en, access on 25.07.2007, 23:43
Kreditkarte.at		http://www.kreditkarte.at	http://www.kreditkarte.at/plb/export/system/Medien/Dokumente/MasterCard/Folder_und_Antrage/Mulitbrand__WERB_business.pdf, access on 07.11.2007, 18:29
Lativian Post		http://info.e-me.lv/en	http://info.e-me.lv/en, access on 15.06.07, 19:42
LG Vocats		http://vocats.com	Le Goeff, Stéphan, Sotiri, Erwin, Getting the deal through: e-commerce, http://vocats.com/index.php?id=170, access on 28.11.2007, 11:19
Macedonski Telekommunicacii		http://www.mt.com.mk/eng	http://www.mt.com.mk/eng/ca/digitalnisertifikati.asp?id=661, access on 01.08.07, 10:54 http://www.mt.com.mk/eng/ca/TipoviNaMTSertifikati.asp?id=679, access on 25.08.07, 12:11
Masterkey		http://www.masterkey.com.ua	http://www.masterkey.com.ua, access on 26.07.2007, 00:18
Meta-Certificate Working Group (MCWG)		http://mcwg.org/mcg-mirror/cert.htm	MCWG, http://mcwg.org/mcg-mirror/cert.htm, access on 10.06.2007, 13:57

Microsec e-Szigno		http://www.e-szigno.hu/index_de.html	http://www.e-szigno.hu/index_de.html, access on 25.07.2007, 19:13
Microsoft		http://www.microsoft.com	Microsoft, QuEST - Qulified Electronic Signatures Tutorial, http://www.microsoft.com/downloads/details.aspx?familyid=0b3c55f6-11d4-4f46-8a37-0ba004e14dcf&displaylang=en, access on 1.10.2007, 9:36
Ministry of Finance of the Czech Republic		http://www.mfcr.cz	Ministry of Finance of the Czech Republic Convergence Programme of the Czech Republic http://www.mfcr.cz/cps/rde/xchg/mfcr/hs.xsl/conv_program_13457.html, access on 25.08.08, 23:43
Ministry of Foreign Affairs of Republic of Armenia		http://www.armeniaforeignministry.am/	http://www.armeniaforeignministry.com/eVisa, access on 27.12.2007, 09:02
Ministry of Foreign Affairs of the Republic of Poland, Information Portal		http://www.poland.gov.pl	http://www.poland.gov.pl, access on 27.06.07, 11:34
Montenegrin Investment Promotion Agency		http://www.mipa.cg.yu	MIPA, Electronic Signature Law, http://www.mipa.cg.yu/pdf/zakoni/Electronic%20Signature%20Law.pfd , access on 09.01.2008, 08:46
National Communication Authority		http://www.nhh.hu/index.php	http://www.nhh.hu/dokumentum.php?cid=10623, access on 28.11.2007, 12:38 http://www.nhh.hu/index.php, access on 08.08.07, 11:41

National IT and Telecom Agency		http://www.itst.dk http://www.signatursekretariatet.dk	http://itst.dk/wimpdoc.asp?page=tema&objno=95024224 , access on 19.07.07, 11:35 http://www.itst.dk/wimpdoc.asp?page=tema&objno=95024223, access on 19.07.07, 11: 46 http://www.itst.dk/publikationer-uk/annual_report_2004/annexes/html/chapter02.htm, access on 22.07.07, 11:25 http://www.signatursekretariatet.dk/certifikatpolitikker.html, access on 22.07.07, 11:02
Norwegian Post and Telecommunication Authority		http://www.npt.no/portal/p	http://www.npt.no/portal/page/portal/PG_NPT_NO_EN/PAG_NPT_EN_HOME/PAG_ABOUT/PAG_ORGANIZATION?menuid=11798 , access on 06.08.07, 11:17
Omnicard		http://www.omnicard.de	http://www.omnicard.de/index.php?m=88&id=1612&suchwort=, access on 18.07.2007, 15:32
OpenLimit		http://www.openlimit.com	OpenLimit, OpenLimit CC Sign 2.1.6.3, https://www.openlimit.com/EN_PROD-OPENLiMiT-CC-Sign.html, access on 1.10.2007, 12:59
Österreichische Apothekerkammer		http://www.apotheker.or.at	http://www.apotheker.or.at, access on 4.12.2007, 19:13
Out-Law		http://www.out-law.com	http://www.out-law.com, access on 11.06.2007, 09:12
PDF Signature		http://www.pdf-signatur.at	PDF Sigantur, Signatur und PDF/A, http://www.pdf-signatur.at/signatur-und-pdfa.html, access on 1.10.2007. 13:12
Politik Digital		http://www.politik-digital.de	Politik-digital.de, Mit digitaler Signatur und Internet-Payment ins virtuelle Rathaus, Expertenchat zum Thema in Kooperation mit NADIV, 25.April 2001, http://www.politik-digital.de/salon/transcripte/sklein.shtml, access on 14.11.2007, 18:13

Post Trust		http://www.post.trust.ie	http://www.post.trust.ie, access on 28.07.07, 15:22 http://www.post.trust.ie/certifid/certifid.html, access on 28.07.2007,15:25 http://www.post.trust.ie/pki/pki.html, access on 28.07.2007, 15:23 http://www.post.trust.ie/reposit/CRL.html, access on 28.07.07, 15:25
Pressetext		http://www.pressetext.at	Pressetext, OpenLimit etabliert mit X.Key Vertriebspartnerschaft für Österreich, Press release 21.1.2008, http://www.pressetext.at/pte.mc?pte=080121020, access on 23.1.2008, 09:12
Price Waterhouse Coopers		http://www.pwc.com	http://www.pwc.com/extweb/industry.nsf/docid/5891e985db830b3c802570c10051f954, access on 01.08.07, 10:24
QuoVadis		http://www.quovadis.ch	http://www.quovadis.ch/page.asp?contentid=22, access on 16.01.2008, 16:04
RISO State Information System		http://www.riso.ee	http://www.riso.ee/en/pub/2003it/p32_s.htm , access on 21.007.2007, 10:44
Romanian National Regulatory Authority for Communication and Information Technology		http://www.anrcti.ro	http://www.anrcti.ro, access on 05.12.2007, 20:27
Rundfunk und Telekom Regulierungs GmbH		http://www.signatur.rtr.at	http://www.signatur.rtr.at/de/providers/services/mobilkom-a1signatur.html, access on 9.11.2007, 15:23
SDU Identification		http://www.sdu-identification.nl	http://www.sdu-identification.nl/eng/frmover.html, access on 04.08.07, 20:36
Security Focus		http://www.securityfocus.com/infocus/1756	Securityfocus http://www.securityfocus.com/infocus/1756, access on 27.06.2007, 12:30

Sigillum PCCE		http://www.sigillum.net.pl	http://www.sigillum.pl/sig-cmsws/page/?F;214, access on 08.08.07, 12:03
SK Certification Authority		http://www.sk.ee	http://www.sk.ee, access on 24.07.2007, 08:45
Skaitmeninio Sertifikavimo Centras		http://www.scs.lt	http://www.scs.lt/?name=menu&act=show&do=13&L=en, access on 06.08.07, 22:35
Stampit		http://stampit.org	http://stampit.org, access on 18.07.07, 19:20
Swisscom, Swiss Digital Certificate Service		http://www.swissdigicert.ch	http://www.swissdigicert.ch/sdcs/portal/page?node=download_ca&sessionid=955bbc9b74f35d3962e110f001df574944cbb186, access on 16.01.2008, 16:13
TACAR -Aerena Academic CA Repository		http://www.tacar.org	ArmeSFo CA - *Certificate Policy and Certification Practice* Statement, Version 0.4, 27 November 2007 https://www.tacar.org/repos/files/Arm_CP_CPS-0.4.pdf
T7EV		http://www.t7ev.org	http://www.t7ev.org/index.php?id=394, access on 14.11.2007, 19:39
TDC Certification Centre		http://tdc.com	http://tdc.com, access on 22.07.07, 11:11 http://tdc.com/publish.php?id=2419, access on 22.07.07, 11:17 http://tdc.com/publish.php?id=2409, access on 22.07.07, 11:16
The Ministry of Informaticn		http://www.micr.cz	http://www.micr.cz/scripts/detail.php?id=3525, access on 15.08.07, 14:17
Thomas Net		http://news.thomasnet.com	http://news.thomasnet.com/companystory/506047, access on 25.07.2007, 23:25
Trans Sped Certification Authority		http://ca.transsped.ro	https://ca.transsped.ro/repository/tscp.pdf, access on 25.07.07, 19:31

Trasury Board of Canada Secretariat		http://www.tbs-sct.gc.ca	Treasury Board of Canada Secretariat, PKI International Scan - December 2004, http://www.tbs-sct.gc.ca/pki-icp/pki-in-practice/efforts/2004/12/scan-analyse06_e.asp, access on 26.06.2007, 22:02
Trust Assured		http://www.trustassured.co.uk	http://www.trustassured.co.uk, 27.06.07, 14:02
TurkTrust		http://www.turktrust.com.tr	http://www.turktrust.com.tr/crl_ain.jsp, access on 25.08.07, 14:25
UK Government Gateway		http://www.gateway.gov.uk	http://www.gateway.gov.uk, access on 18.12.2007, 13:34
Unizeto Technologies		http://www.unizeto.pl	http://www.unizeto.pl/unizeto/uni,aboutus_about_company.xml, access on 08.08.07, 12:01 http://www.unizeto.pl/unizeto/uni,offer_pki_software.xml, access on 07.08.07, 23:02
VeriSign France SAD		http://www.verisign.fr	http://www.verisign.fr/ssl/index.html, access on 14.11.2007, 19:47
Visualbuilder		http://www.visualbuilder.com	http://www.visualbuilder.com/viewnews.php?group_id=15&news_id=633, access on 26.06.2007, 19:39
VUB Banka		http://www.vub.sk	http://www.vub.sk/en/show.asp?category=1953, access on 10.08.07, 19:08
Wirtschaftuniversität Wien		http://www.wu-wien.ac.at/	http://e-voting.wu-wien.ac.at/scripts/download.php?F_ID=72, access on 07.11.2007, 19:54
WKO Austria		http://portal.wko.at	http://portal.wko.at/wk/sn_detail.wk?AngID=1&DocID=363836&StID=187037, access on 14.11.2007, 16:11 http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=313671&DstID=0&BrID=513, access on 14.11.2007, 16:11

Appendix

Appendix A: German Abstract

Heutzutage leben wir in einer e-Area: eBusiness, eCommerce, eBanking und weitere Begriffe prägen unser alltägliches Leben. Ohne iese Stichworte ist unsere Gesellschaft und Wirkschaft nicht mehr vorstellbar. Die Technologie Internet hat diese Schlagworte ermöglicht und vorangetrieben und bietet eine reihe von Möglichkeiten, Vor- aber ebenso Nachteile.

Über 250 Million Europäer nutzen das Internet regelmäßig, 80% davon via Breitbandverbindung. In Europa, 60% der öffentlichen Services sind online zugänglich. Informations- und Kommunikationsnetzwerke sind von großer Wichtigkeit in unserer Gesellschaft und ermöglichen Bürgern und Unternehmen gemeinsam und mit öffentlichen und privaten Einrichtungen und Institutionen zu kommunizieren.

Eine Herausforderung birgt das Thema der Anonymität der Nutzer des World Wide Webs und verursacht oft Probleme im Bereich der Authentifizierung und Integrität. Sicherheit von elektronischer Kommunikation und von Transaktionen ist ein kritisches Thema heutzutage. Der Anteil von Transaktionen, die im Cyberspace ausgeführt werden steigt graduell. Die elektronische Form ersetzt nach und nach das Papier.

Eine Barriere in eCommerce und eCommunication ist, dass ein Gegebüber nicht gesehen werden kann und seine Identität nicht überprüft werden kann (via Passport oder ID-Karte). Um jedoch einen Vertrag abzuschließen, ein hoher Sicherheitsstandard ist notwendig um einerseits festzustellen, dass der Vertragspartner auch derjenige ist, für den er sich ausgibt, und weiters um sich abzusichern, dass der unterschriebene Vertrag nicht nachträglich abgeändert wird.

Um in diesem heiklen Bereich die Vorteile elektronischer Medien zu nutzen und davon zu profitieren wurde die elektronische Signatur entwickelt. Das Thema „Digitale Signatur ist ein damit ein integrativer Bestandteil jeder digitalen Geschäftsdurchführung. Vertragspartner haben die Möglichkeit sich zu identifizieren und gültige Willenserklärungen abzugeben. In diesem Zusammenhang ist es wichtig auf Internet Sicherheit und Risikovermeidung hohen Wert zu legen. Aus diesen Gründen widmete ich diesem Thema hohe Aufmerksamkeit und stieß auf das Thema der digitalen Signatur, einem integrativen Teil digitaler Transaktion.

Da sich auch Unternehmen, im Speziellen vor allem im Bereich des eCommerce und eBusiness Sektors mit der Sicherheit digitaler Transaktionen auseinandersetzen, wurde diese Studie innerhalb eines Projektes mit dem Forschungsverein E-Commerce Competence Center (EC3) in Wien erstellt. Durch die Kooperation mit EC3 wurde es mir ermöglicht, Synergien auszuschöpfen und ein internationales

Netzwerk von Kontakten aufzubauen. Hier muss ausdrücklich darauf hingewiesen werden, dass ich die Alleinautorenschaften der Studie innehabe.

Ein Projekt im Bereich der digitalen Signatur beschäftigt sich mit der grenzüberschreitenden Anwendung digitaler Signatur, welche den europäischen Raum umfasst. Basierend auf ersten Untersuchungen wurde ersichtliche, dass eine globale Zusammenschau auf Europäischer Ebene nicht existiert. Daher habe ich mich bemüht, eine strukturierte Zusammenschau in drei Dimensionen zu erarbeiten: rechtliche Rahmenbedingungen, technische Standards und Marktdurchdringung.

In diesem Zusammenhang wurden folgende Länder untersucht (siehe nachfolgende Tabelle: Untersuchte Länder):

Tabelle: Untersuchte Länder, Quelle: eigene Darstellung

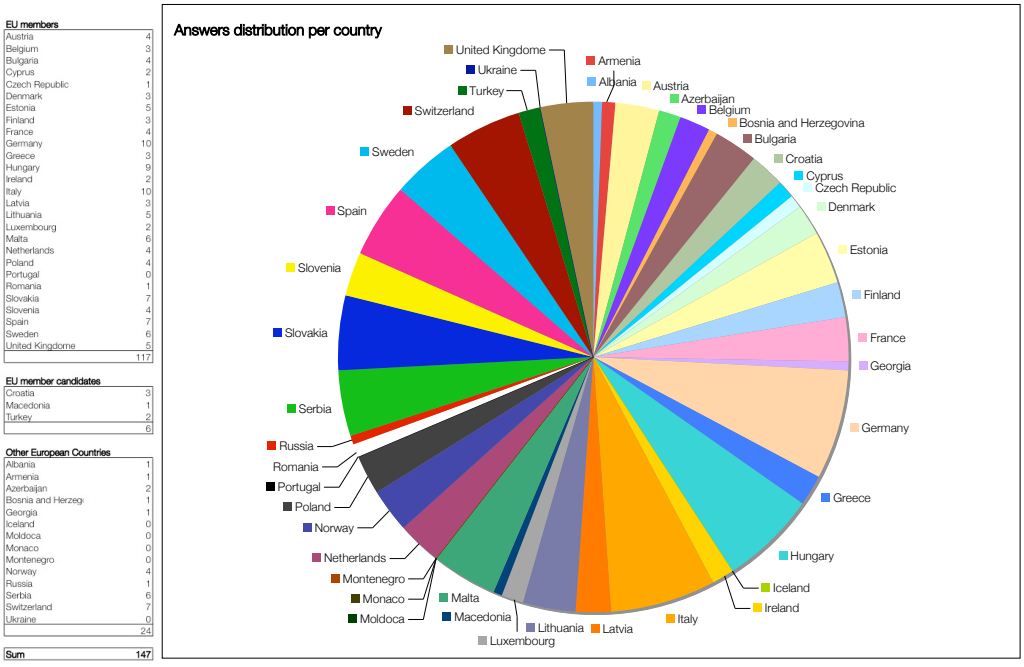
EU Mitgliedsstaaten		
Belgien	Italien	Rumänien
Bulgarien	Lettland	Schweden
Dänemark	Littauen	Slovakei
Deutschland	Luxemburg	Slovenien
Estland	Malta	Spanien
Finland	Niederlande	Tschechien
Frankreich	Österreich	Ungarn
Griechenland	Polen	Vereinigtes Königreich
Irland	Portugal	Zypern
EU Bewerberländer		
Kroatien	Mazedonien	Türkei
Andere Europäische Staaten		
Albanien	Island	Russland
Armenien	Moldavien	Serbien
Azerbaijan	Monaco	Schweiz
Bosnia Herzegovina	Montenegro	Ukraine
Georgien	Norwegen	

Um einen allgemeinen Eindruck über die aktuelle Situation in jedem Land zu gewinnen, wurde eine erste Internetrecherche gestartet. Offizielle Länderseiten, Informationsseiten von Außenministerien und öffentlichen Einrichtungen, sowie Homepages von IT- und Kommunikationsunternehmen werden

aufgerufen um allgemeine Informationen sowie Kontaktadressen einzuholen.
Um detaillierte Informationen zu beschaffen wurde die Wirtschaftskammer sowie verschiedene Ministerien jedes Landes per E-Mail oder telefonisch kontaktiert.

Weiters wurde ein Fragenkatalog zusammengestellt und per e-Mail ausgesandt.
Insgesamt wurden während der Erstellung der Studie 661 Emails versandt, circa 22% Antworten wurden von verschiedenen Firmen und Behörden beantwortet: Bei Abschluss der Studie wurden 144 Fragebögen beantwortet via E-Mai Korrespondenz. Dies kann als beachtliche Zahl angesehen werden wenn man die Komplexität der Studie betrachtet. Die Ergebnisse können als repräsentativ angesehen werden, da die Antworten durch Spezialisten im Bereich der elektronischen Signatur gegeben wurden. Eine Liste aller Korrespondenzen befindet sich im Anschluss an die Studie.

Die Geografische Lage der Korrespondenzen betrachtend wird ersichtlich, dass die Antworten weit verstreut in Europa und darüber hinaus liegen: von 147 Antworten, 117 Antworten wurden von EU Mitgliedsstaaten, 6 Antworten von den 3 EU-Bewerberländer und 24 Antworten von den 14 anderen Europäischen Ländern zurückgesandt (siehe nachfolgende Abbildung: Verteilung der Antworten nach Ländern).



EU members	
Austria	4
Belgium	3
Bulgaria	4
Cyprus	2
Czech Republic	1
Denmark	3
Estonia	5
Finland	3
France	4
Germany	10
Greece	3
Hungary	9
Ireland	2
Italy	10
Latvia	3
Lithuania	5
Luxembourg	2
Malta	6
Netherlands	4
Poland	4
Portugal	0
Romania	1
Slovakia	7
Slovenia	4
Spain	7
Sweden	6
United Kingdome	5
	117

EU member candidates	
Croatia	3
Macedonia	1
Turkey	2
	6

Other European Countries	
Albania	1
Armenia	1
Azerbaijan	2
Bosnia and Herzegi	1
Georgia	1
Iceland	0
Moldoca	0
Monaco	0
Montenegro	0
Norway	4
Russia	1
Serbia	6
Switzerland	7
Ukraine	0
	24

Sum	147

Abbildung: Verteilung der Antworten nach Ländern, Quelle: eigene Darstellung

Einige der versandten E-Mail konnten den Empfänger nicht erreichen (17%). Gründe dafür waren, dass einige E-Mail Kontakte nicht mehr gültig waren, oder der Empfänger sich „out of office“ befand (z.B. auf Urlaub).

Die eingeholten Informationen wurden in der Studie zusammengefasst. Zum Zweck der Übersichtlichkeit wurde die Studie stark Strukturiert und subjektive Interpretationen bewusst ausgelassen um die Fakten für sich sprechen zu lassen.

Eine gewisse Verzerrung der Ergebnisse bei der Betrachtung eines Länderprofils kann nicht ausgeschlossen werden. In manchen Ländern war die Suche nach Daten oft aufgrund von Sprachbarrieren erschwert, und nur wenig brauchbare Information verfügbar. Dies schließt jedoch nicht aus, dass mehr Datenmaterial existiert. Trotz großer Bemühungen, Lücken in jenen Ländern zu füllen, in denen Informationen rar waren, war die Suche mühsam und das Ergebnis teilweise nicht zufriedenstallend. Der Aufwand wurde intensiviert aber nicht von entsprechenden empirischen Ergebnissen begleitet. Diese Heterogenität der Daten kann eventuell einen falschen Eindruck fördern.

Die Vollständigkeit der gesammelten Daten wird reflektiert in der Länderklassifikation.
Um einen raschen Überblick zu erlangen wurde am Ende jeder Länderanalyse eine Tabelle erstellt, welche die Entwicklung des Landes in Bezug auf digitale Signaturstandards zusammenfasst, sowie eine Bewertung in Hinblick auf verfügbare Information und Entwicklungsstand enthält.
Diese Bewertung ist veranschaulicht durch zwei Arten der Wertentwicklung:

a) Farbe

Die Farbe verdeutlicht, wie viel Informationsmaterialien gefunden wurden und wie viel Information durch Korrespondenzen eingeholt werden konnte (siehe nachfolgende Tabelle: Bedeutung der farblichen Bewertung).

Tabelle: Bedeutung der farblichen Bewertung, Quelle: eigene Darstellung

Farbe	Bedeutung
	viel Information vorhanden
	mäßig Information vorhanden
	wenig Information vorhanden

b) Buchstaben
Die Bewertung durch Buchstaben erfolgte durch eine Dreierreihung. Die erste Position steht für die rechtlichen Rahmenbedingungen, die zweite für die technischen Standards und die dritte Position bezeichnet die Marktdurchdringung elektronischer Signatur.
Um den Status jedes Landes auszudrücken wurden die Buchstaben A, B und C verwendet (siehe nachfolgende Abbildung: Erklärung der Bewertung mit Buchstaben).

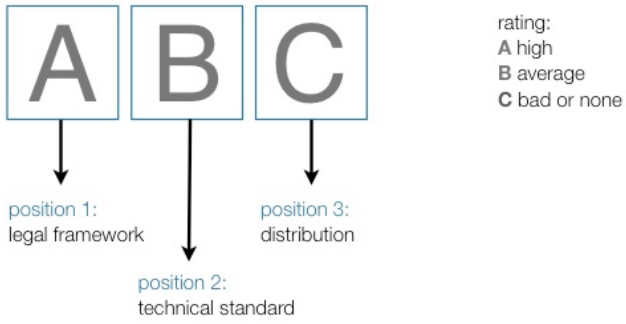


Abbildung: Erklärung der Bewertung mit Buchstaben, Quelle: eigene Darstellung

AAA bedeutet, dieses Land verfügt über einen fundierten rechtlichen Rahmen, hoch entwickelte technische Standards sowie über einen hohen Verbreitungsgrad von elektronischen Signaturanwendungen.
CCC bedeutet, das Land befindet sich in schlechter Ausgangslage, sowohl rechtlich, technisch als auch die Verbreitung von Anwendungen und Systemen betreffend.

Am Ende der Studie wurde eine Gesamttabelle erstellt, welche einen Gesamtüberblick über alle zentralen Fakten ermöglicht, getrennt nach den drei Kategorien rechtliche Rahmenbedingungen, Voraussetzungen für den Einsatz digitaler Signatur und Technisches Umfeld für elektronische Signatur.
Die Spalte ganz rechts gibt die angewandte drei-Buchstaben- sowie die Farbbewertung wieder.

Bei genauerer Betrachtung der Abschlusstabelle kann viel Dynamik beobachtet werden.

Die Europäische Kommission hat ein Gemeinschaftsframework für elektronische Signatur geschaffen (Europäische Richtlinie für digitale Signatur 1999/93/EC). Das Ziel war, einen Rahmen für den Gebrauch von elektronischer Signatur zu schaffen und eine grenzüberschreitende Anwendung von Produkten und Systemen zu ermöglichen.
In den EU-Mitgliedsstaaten wurden große Anstrengungen unternommen um rechtliche Rahmenbedingungen für elektronische Dokumente und digitale Signatur zu schaffen und einen Markt für solche Applikationen zu etablieren. Die meisten Initiativen wurden in den Jahren von 2000 - 2001 unternommen, doch seit daher wurde wenig unternommen. Dies verschafft den Eindruck, dass die „high times“ in diesen Ländern bereits vorbeigezogen sind. Hier wird auch wenig Aktivität in den nächsten Jahren erwartet.

Im Gegensatz dazu befinden sich die verbleibenden untersuchten Länder nicht auf dem selben Stand der Entwicklung. Obwohl die rechtlichen Rahmenbedingungen bereits in fast jedem Land zur Gänze umgesetzt wurde, stehen die rechtlichen Regelungen und die technische Implementierung auf einem Balanceakt. In manchen Ländern herrscht eine beinahe unhandbare Vielfalt von technischen Standards und Applikationen.

Die aktuelle Studie demonstriert auf deutliche Art und Weise, dass es keine globale Implementierung von digitaler Signatur bis jetzt erreicht wurde, hauptsächlich durch eine technische Interoperabilität der Systeme, Prozesse und Konfigurationen, wobei die rechtlichen Rahmenbedingungen nicht das Hindernis sind. Es ist nicht schwer zu verstehen, dass eine grenzüberschreitende Adoption der digitalen Signatur nicht auf dies Art und Weise realisierbar ist.

In vielen Ländern erreicht die qualifizierte elektronische Signatur den selben rechtlichen Status wie eine händische Unterschrift. Dennoch wird sie in einigen Ländern nur teilweise rechtliche geregelt (zum Beispiel in Estland oder Slowakei), oder elektronische Signatur wird überhaupt nicht anerkannt (Bulgarien).

Auf technischer Seite hat die Europäische Richtlinie einen Einfluss auf viele international Initiativen zur Standardisierung und Harmonisierung genommen und viele Aktivitäten veranlasst, die die Entwicklung und Verbesserung von Online-Services, eGovernment und Anwendungen elektronischer Signatur fördern.

Das World Market Research Center untersuchte eGovernmentanwendungen von 196 Staaten weltweit. Dabei schnitt Europa nicht besonders gut ab und erreichte nur 34,1% der Gesamtpunkte, da europäische Seiten über nicht viele relevanten Funktionen verfügen. Das Ranking der Studie kann im Anhang Appendix 45 - Miscellaneaous eingesehen werden.
Datensicherung und -wahrung ist von großem Interesse, aber viele Webseiten vernachlässigen es, den Bürger über Datenschutz und Sicherheitsbestimmungen zu informieren Auch die Nutzbarkeit von Seiten für behinderte Personen verfehlte die Ziele von vielen Initiativen. Weiters fehlt oft die Möglichkeit, via Kreditkare oder elektronische Signatur Zahlungen vorzunehmen.

Einige Länder starteten Initiativen für den Einsatz von elektronischen Ausweisen und entwickelten eID Karten, welche elektronische Zertifikate für Authenifizierung und digitale Signatur speichern.
EU Mitgliedsstaaten wie Belgien, Italien, Estland oder Spanien haben eID Karten ausgegeben, andere Länder planen die Einführung der Karten(Portugal plant den Start der Einführung für 2008).

Aber auch die Adoption von eSignatur Anwendungen hat einige Schwierigkeiten aufgeworfen. Ein großes Hindernis für die Akzeptanz und den Einsatz elektronischer Signatur ist das Fehlen von Interoperabilität von Systemen und Applikationen, sowohl national als auch grenzüberschreitend. Zum Beispiel akzeptieren einige Applikationen nur Zertifikate eines bestimmten Zertifizierungsdienstleisters.
Ein großes Problem stellt auch die fehlende Transparenz dar, die Unsicherheit in den Markt bringt, wie über bestehende Signaturstandards oder rechtliche Voraussetzungen.

Um die Verwendung von elektronischer Signatur voranzutreiben hat die europäische Kommission in Kooperation mit eineigen privaten Institutionen eine reihe an Initiativen gestartet. Weiters will die Kommission auch weiter Standardisierungsmaßnahmen vorantreiben um eine nationale und grenzüberschreitende Interoperabilität und Anwendung von eSignatur-Systemen zu unterstützen und zu ermöglichen.

Aufgrund der immer mehr zunehmenden Verbreitung von elektronischen Ausweisen und der Adoption elektronischer Signatur in der elektronischen Administration (wie eTaxing) kann angenommen werden, dass die Nachfrage von elektronischer Signatur zunehmen wird. Die Europäische Richtlinie 1999 wird dabei als solide rechtliche Grundlage für eine Einführung und die Verwendung von elektronischer Signatur dienen.

Zusätzlich müssen die Europäische Kommission und andere Institutionen die Verwendung von eSignatur bewerben und den privaten und öffentlichen Beriech dazu reizen, die Vorteile der elektronischen Signatur in Anspruch zu nehmen und zu nutzen.
Weiters wird gehofft, dass diese Studie durch das Aufzeigen der aktuellen Situation in Europa wesentlich dazu beiträgt, die Idee der digitalen Signatur zu fördern.

Appendix B: Curriculum Vitae

Curriculum Vitae

Carina Isabella Freudenthaler

Franz Binder-Str. 43
A-3100 St. Pölten
Tel.: 0699 / 11706997
Email: carinaisabella@gmx.at

Geburtsdatum: 31.März 1984
Geburtsort: Wien
Familienstand: ledig, keine Kinder

Ausbildung

seit 10/2002	Studium der Internationalen Betriebswirtschaft, Universität Wien *Wirtschaftssprachen*: Englisch, Französisch *Schwerpunkt*: eBusiness Innovations- und Technologiemanagement Wirtschaftsinformatik *Diplomarbeit*: International Study: „State of the Art of Electronic Signatures - Evaluation in 44 Nations“
1994 - 2002	Gymnasium der Englischen Fräulein, 3100 St. Pölten Abschluss durch Matura mit ausgezeichnetem Erfolg *Maturafächer:* Deutsch, Englisch, Mathematik, Informatik, Psychologie, Bildnerische Erziehung

Universitäre Projekte

WS 2007 / 2008	Mitarbeit am Fachbereich Electronic Business der Universität Wien, Fakultät für Wirtschaftswissenschaften, Mitwirkung bei fachlichen Diskussionen über neue Technologien und Medien, Vorträge über Forschungsschwerpunkte des Fachbereichs http://www.univie.ac.at/ebusiness
SS 2007	Im Rahmen des Seminars “Neue Entwicklungen im eBusiness”, Kernfachkombination eBusiness, in Kooperation mit dem Kompetenzzentrum E-Commerce Competence Center in Wien, Mitarbeit am Innovationsprojekt “EasySign”, Durchführung einer internationalen Studie zur Entwicklung einer Plattform zur grenzüberschreitenden Nutzung qualifizierter digitaler Signaturen im Bereich des eProcurement http://www.ec3.at
SS 2007	Teilnahme im Team der Universität Wien am hochschulübergreifenden Wettbewerb technischer und wirtschaftlicher Studiengänge „Accenture Campus Challenge 2007“ zum Thema „Wireless Sensor Networks“, Zuständig für das Coorporate Design, Präsentation und Bau des Prototypen http://www.univie.ac.at/itm/events/campuschallenge07.htm http://careers3.accenture.com/Careers/ASGCampusChallenge

SS 2007	5. März 2007: Einladung zur eBusiness Class der Österreichischen Computer Gesellschaft, Präsentation der Arbeit aus der Lehrveranstaltung "Einführung ins eBusiness", Thema: „Ganz in Weiß – Konzeption eines eBiz Start-up Unternehmens" http://www.ocg.at/ak/ebusiness/archiv.html http://www.ocg.at/ak/ebusiness/files/ebusinessclass_oj.pdf
WS 2006 / 2007	Im Rahmen der LV „Applications of Innovation and Technology Management", Kernfachkombination Innovations- und Technologiemanagement, in Kooperation mit der TU Wien, Durchführung einer Markterhebung zum Thema: BioFit - Synthesekraftstoffe aus Biomasse

Berufserfahrungen

05/2007 - 06/2008	EC3 – E-Commerce Competence Center Researcher - Forschungsbereich dBiz - Digital Business Research, Development and Innovation Management http://www.ec3.at/ http://dbiz.ec3.at/ http://www.univie.ac.at/itm/events/ec3_standard05.htm Mitarbeit im Innovationsprojekt "EasySign", Durchführung einer internationalen Studie zur Entwicklung einer Plattform zur grenzüberschreitenden Nutzung qualifizierter digitaler Signaturen im Bereich des eProcurement „European Study of Electronic Signature", Durchführung einer internationale Studie über die grenzüberschreitende Anwendung digitaler Signatur im Europäischen Wirtschaftsraum in den Dimensionen rechtliche Rahmenbedingungen, technische Standards und Marktdurchdringung, Aufbau eines internationalen Netzwerks
10/2005 – 11/2005	One-World SCS, Wien-Vösendorf Promotion und Kundenberatung
03/2003 – 10/2005	DocLX Event Consulting GmbH, 1190 Wien Unifestpromotion, Organisation der Plakatierung und Flyerverteilung
04/2003 – 12/2004	Easy Drivers, Fahrschule Graf, 3100 St. Pölten Unterstützung der Geschäftsführung, Kundenbetreuung und -beratung,
07/2003 – 07/2003	BüroV, Jugend-, Kultur- und Veranstaltungsmanagement, 3100 St. Pölten St. Pöltner Hauptstadtfest, Mitarbeit im Organisationsteam, Künstlerbetreuung
05/2003 – 05/2003	BüroV, Jugend-, Kultur- und Veranstaltungsmanagement, 3100 St. Pölten „500 Jahre Rathaus"-Feier, Mitarbeit im Organisationsteam, Gästebetreuung
07/2001 – 08/2001	Niederösterreichische Gebietskrankenkasse, 3100 St. Pölten Ferialpraxis,

07/2001 – 07/2001	BüroV, Jugend-, Kultur- und Veranstaltungsmanagement, St. Pöltner Hauptstadtfest, Mitarbeit im Organisationsteam, Künstlerbetreuung
07/2000 – 08/2000	Niederösterreichische Gebietskrankenkasse, 3100 St. Pölten Ferialpraxis

Ehrenamtliche Tätigkeiten

2004	Reit- und Zuchthof Wultendorf, 3385 Markersdorf Mitarbeit bei Reitercamps im Sommer 2004, Kinderbetreuung, Voltigierunterricht
2000 - 2002	„Joynt – the youth mag", Jugendmagazin für den Großraum St. Pölten Redaktionstätigkeit inklusive Photoredaktion
	Jugendzentrum Steppenwolf, 3100 St. Pölten Mitorganisation und Mitarbeit bei einer Jugendveranstaltung
2000	Mitarbeit bei dem Benefizprojekt „Mary Ward 2000 – Mädchenschule für Pakistan", Gymnasium der Englischen Fräulein St. Pölten Aushilfe in der Fahrschule Graf St. Pölten

Sprachen

Latein – Maturaniveau
Englisch – fließend in Wort und Schrift
Französisch – gut in Wort und Schrift

Besondere Kenntnisse

Führerschein der Klassen A und B
Betriebssystem Windows, Mac OS
MS Office Pakete, Photoshop, Adonis

Interessen / Hobbys

Erschließung neuer Themenbereiche,
innovative IT-Lösungen, neue Medien
Management und Organisation, Kundenbetreuung
Fotografie, Grafik, Design, Malerei, Schauspiel
Sportliche Betätigung (Reiten, Schwimmen, Tennis)