universität wien

DISSERTATION

Titel der Dissertation

Die neuen rechtlichen und technischen Rahmenbedingungen der behördlichen elektronischen Zustellung

Verfasser

MMag. Dipl.-Ing. Bernhard Horn

angestrebter akademischer Grad

Doktor der Rechtswissenschaften (Dr. iur.)

Wien, 2012

Studienkennzahl lt. Studienblatt:	A 083 101
Dissertationsgebiet lt. Studienblatt:	Rechtswissenschaften
Betreuer:	Ao. Univ.-Prof. Dr. Wolfgang ZANKL

Meinen Eltern

Inhaltsverzeichnis

1. Einleitung

Ein zentrales Element der hoheitlichen Tätigkeit von Verwaltungsbehörden und Gerichten ist die Übermittlung von Erledigungen an den betroffenen Rechtsunterworfenen. Wird die Behörde mit einer Angelegenheit befasst, welche ihrem Zuständigkeitsbereich zuzuordnen ist, so hat sie diese in einem gesetzlich geregelten Verfahren und im ihr vom Gesetz eingeräumten Ermessen zu erledigen. In einem solchen Verfahren hat die Behörde üblicherweise einen konkreten hoheitlichen Willen zu bilden, wie die Sache zu erledigen ist, und kann auf Grund des ihr gesetzlich eingeräumten Imperiums für Rechtsunterworfene verbindliche Anordnungen treffen, Rechtsmacht ausüben oder die Rechtslage gestalten. Damit solche Anordnungen Rechtswirksamkeit entfalten und dem Betroffenen die Möglichkeit eingeräumt wird, sich entsprechend dieser Anordnung zu verhalten, muss ihm der Inhalt einer solchen Anordnung zur Kenntnis gebracht werden. Dies kann entweder unmittelbar durch direkte mündliche Bekanntgabe (zB bei Anwesenheit oder per Telefon) oder durch Zustellung einer schriftlichen Ausfertigung erfolgen. Als Erledigung ist folglich jeder Akt zu verstehen, den die Behörde nach außen hin setzt.[1] In Frage kommen dafür beispielsweise Bescheide, Urteile oder eben auch rein faktische Handlungen wie die Ausstellung und Aushändigung eines beantragten Reisepasses.

Für Verwaltungsbehörden, die ihre Verfahren gemäß dem EGVG nach dem AVG zu führen haben, besteht für die Form der Erledigung weitgehend Formfreiheit (§ 18 Abs 1 AVG). Das bedeutet, dass diese mündlich, schriftlich oder auch in jeder anderen technisch möglichen Form ergehen kann, jedoch ist eine Erledigung immer dann schriftlich auszufertigen, wenn dies ausdrücklich gesetzlich angeordnet ist oder von einer Partei verlangt wird (§ 18 Abs 2 AVG). Damit eine Erledigung rechtliche Wirksamkeit erlangen kann, muss sie dem Betroffenen bekannt gegeben werden, was bei schriftlichen Erledigungen durch Zustellung einer Fertigung in Form eines behördlichen Dokuments[2] erfolgt. Für die Zustellung einer solchen Fertigung ist das Zustellgesetz (ZustG[3]) anwendbar (§§ 1 ZustG, 21 AVG). Zu beachten ist jedoch, dass im Bereich der Gerichte das ZustG nur für die Zustellung physischer Dokumente anwendbar ist, für die Zustellung elektronischer Dokumente kommen die §§ 89a ff Ge-

[1] Vgl *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 130.
[2] Vgl die Legaldefinition „Dokument" in § 2 Z 2 ZustG.
[3] BGBl I 200/1982 idF BGBl I 111/2010.

richtsorganisationsgesetz (GOG) zur Anwendung (§ 28 Abs 2 ZustG), also der Elektronische Rechtsverkehr der Gerichte (ERV)[4].

1.1 Entwicklung und Aufbau des ZustG

Ursprünglich waren die Regelungen über die Zustellung verwaltungsbehördlicher Dokumente im 4. Abschnitt des AVG angesiedelt, wurden aber mit dem BGBl I 200/1982 in ein eigenes Gesetz mit dem Langtitel *„Bundesgesetz vom 1. April 1982 über die Zustellung behördlicher Schriftstücke (Zustellgesetz)“* ausgegliedert. Dieses trat mit 1. 3. 1983 in Kraft. In späterer Folge wurden zusammen mit dem E-Government-Gesetz (E-GovG) auch die Bestimmungen des Zustellgesetzes durch das BGBl I 10/2004 umfassend novelliert und ein neuer III. Abschnitt mit den Regelungen zur elektronischen Zustellung von Dokumenten eingefügt. Die nächste Novelle, mit welcher Anpassungen bezüglich der elektronischen Kommunikation zwischen Bürgern und Behörden umgesetzt wurden, erfolgte durch das Verwaltungsverfahrens- und Zustellrechtsänderungsgesetz 2007 (BGBl I 5/2008). Die letzte Novellierung erfolgte durch das Budgetbegleitgesetz 2011 (BGBl I 111/2010), mit welchem die Möglichkeit vorgesehen wurde, dass Dokumente, die bei einem elektronischen Zustelldienst eingelangt sind, von diesem an den ERV weitergeleitet werden können.

1.2 Anwendungsbereich des Zustellgesetzes

Für die Zustellung verwaltungsbehördlicher oder gerichtlicher Dokumente ist das Zustellgesetz anwendbar, sofern es sich um solche Dokumente handelt, welche in Vollziehung der Gesetze – also im Zuge der Hoheitsverwaltung – an einen Rechtsunterworfenen zu übermitteln sind (§ 1 ZustG). Das bedeutet, dass nicht jede Übermittlung eines Schriftstücks bzw Dokuments an eine natürliche oder juristische Person dem Regelungsregime des ZustG unterliegt, sondern lediglich solche, durch welche die Behörde dem Rechtsunterworfenen mit Hoheitsgewalt (Imperium) gegenüber tritt. Mit den Regelungen des Zustellgesetzes versucht der Gesetzgeber einen gewissen Ausgleich zwischen widerstreitenden Interessen zu finden: Einerseits soll der von einem behördlichen Rechtsakt betroffenen Person der Inhalt dieses Rechtsakts zur Kenntnis gebracht werden, andererseits sollen die Rechtswirkungen auch dann eintreten, wenn der betroffenen Person – aus welchem Grund auch immer – die Existenz oder der Inhalt dieses Rechtsakts tatsächlich nicht zur Kenntnis gelangte. Unter

[4] Vgl http://www.help.gv.at/Content.Node/99/Seite.991099.html, abgerufen am 17. 1. 2012.

dem Begriff „Zustellung“ ist somit nur die Übermittlung behördlicher Dokumente im Zuge der Hoheitsverwaltung zu verstehen, nicht jedoch die Übersendung von Dokumenten im Zuge der Privatwirtschaftsverwaltung oder zwischen Behörden.[5]

Da die Regelungen des ZustG bezüglich der elektronischen Zustellung nicht für die Zustellung gerichtlicher Dokumente anwendbar sind (§ 28 Abs 2 ZustG), fokussieren sich die Ausführungen in dieser Arbeit lediglich auf den Bereich der Verwaltung.

1.3 Das Verwaltungsverfahren nach dem AVG

Wie eingangs dargelegt, stellt die Zustellung behördlicher Dokumente im Allgemeinen einen integralen Bestandteil der Durchführung von Verwaltungsverfahren dar. Ein Verwaltungsverfahren nach dem AVG gliedert sich regelmäßig in folgende Teilschritte:

- **Verfahrenseinleitung**: durch Anbringen eines „Einschreiters“ oder von Amts wegen
- **Ermittlungsverfahren**: Erhebung des rechtserheblichen Sachverhalts
- **Erledigung**: formale Willensbildung und –äußerung durch die Behörde
- **Zustellung**: dem Betroffenen wird die behördliche Entscheidung schriftlich zur Kenntnis gebracht.

Da sich diese Arbeit auf die elektronische Zustellung von Dokumenten im Bereich der Verwaltung konzentriert, wird im Folgenden kurz dargelegt, welche Möglichkeiten die österreichische Rechtsordnung vorsieht, um die Durchführung von Verwaltungsverfahren mit elektronischen Hilfsmitteln zu unterstützen. Ein im österreichischen E-Government angestrebtes Ziel ist die vollständige elektronische und damit medienbruchfreie Abwicklung behördlicher Verfahren.

Die nachfolgende Grafik stellt den österreichischen E-Government-Musterprozess dar und zeigt sehr anschaulich, wie ein durchgängig elektronisch geführtes Verwaltungsverfahren beispielhaft aussehen könnte: Am Beginn steht das Anbringen eines Bürgers, welches in elektronischer Form und mittels Bürgerkarte digital signiert und anschließend bei der Behörde eingebracht wird. Nach Prüfung der Signatur wird der

[5] Vgl *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 353, mwN.

Bearbeitungsprozess (das Ermittlungsverfahren) intern angestoßen, welcher ggf durch ein elektronisches Akten- bzw Workflowmanagementsystem („ELAK-System“) unterstützt werden kann. Am Ende wird die Erledigung elektronisch verfasst, von der Behörde bzw dem Sachbearbeiter (digital) unterschrieben und dem Empfänger elektronisch zugestellt.[6]

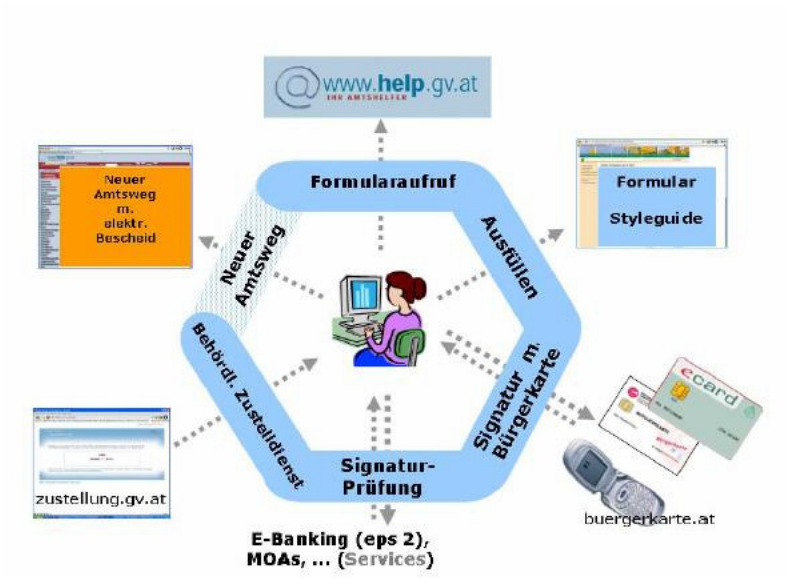

Abbildung 1: Der E-Government Musterprozess[7]

1.3.1 Anbringen

Ein Verwaltungsverfahren nach dem AVG kann entweder durch ein Anbringen von einem Rechtsunterworfenen gem § 13 AVG durch Antrag, Gesuch, Anzeige, Beschwerde und sonstige Mitteilung bzw amtswegig durch die Behörde selbst (§ 39 AVG) initiiert werden. Anbringen als Anstoß für ein Verwaltungsverfahren können gem § 13 AVG von Bürgern mündlich, telefonisch, schriftlich oder in jeder anderen technisch möglichen Form – also auch elektronisch – bei der Behörde eingebracht werden. „Technisch möglich“ iSd § 13 Abs 2 AVG bedeutet in diesem Zusammenhang, dass die Behörde die entsprechende technische Infrastruktur für den Empfang von Anbringen in dieser technischen Form bereits geschaffen haben muss (zB Betrieb eines E-Mail-Systems, Postfach bei einem elektronischen Zustelldienst, Anbindung an einen Formularserver[8], etc). Bürger haben jedoch keinen Anspruch darauf, dass bestimmte technische Möglichkeiten für die Einbringung von Anbringen von der

[6] Vgl *BKA*, Behörden im Netz, 102 f.
[7] *BKA*, Grundlagen zum österreichischen E-Government Gütesiegel, 8.
[8] Vgl Formularserver des Landes Steiermark, http://www.e-government.steiermark.at/cms/ziel/2221039/DE, abgerufen am 17. 1. 2012.

Behörde geschaffen werden.[9] Die von einer Behörde bereitgestellten Kommunikationskanäle, die technischen und organisatorischen Voraussetzungen für deren Benützung sowie etwaige technische oder organisatorische Beschränkungen sind im Internet kund zu machen (zB auf der Behördenhomepage) und vom Einschreiter für die Rechtswirksamkeit einer (elektronischen) Kommunikation mit der Behörde zu beachten. Dies bezieht sich beispielsweise auch auf E-Mail-Adressen, bei welchen Anbringen eingebracht werden können, oder bestimmte Dateiformate, die die Behörde zu empfangen bzw zu verarbeiten in der Lage ist. Die Missachtung solcher Anordnungen führt zu einem Mangel des Anbringens, der auch nicht gem § 13 Abs 3 AVG verbesserungsfähig ist.[10] Anbringen via E-Mail sind nur dann zulässig, wenn die Behörde für die Einbringung von Anbringen nicht besondere Übermittlungsverfahren vorgesehen hat, wie zB (elektronisch zu signierende) Online-Formulare oder Einkommensteuererklärungen über FinanzOnline[11].

Im Umkehrschluss aus § 13 Abs 4 AVG, der bei Zweifeln über die Identität des Einschreiters oder die Authentizität des Anbringens die Behörde verpflichtet einen Verbesserungsauftrag gem Abs 3 aufzutragen, ergibt sich, dass schriftliche Anbringen nicht notwendigerweise mit einer Unterschrift versehen werden müssen. Ein solcher Nachweis der (eindeutigen) Identität (§ 2 Z 1 oder Z 2 E-GovG) und Authentizität (§ 2 Z 5 E-GovG) ist jedoch dann erforderlich, wenn sich dies aus einer gesetzlichen Bestimmung[12] ergibt oder die Behörde dies aus Ermessensgründen für notwendig erachtet. Auch welchen Grad des Identitätsnachweises (eindeutig/nicht eindeutig) sie fordert, obliegt den konkreten Umständen entsprechend ihrem Ermessen. Die eindeutige Identität und Authentizität eines Anbringens kann im elektronischen Verkehr mit der Behörde beispielsweise durch Einsatz der Bürgerkarte (§ 2 Z 10 E-GovG) nachgewiesen werden (vgl Kapitel 5). Insbesondere im elektronischen Verkehr darf eine solche Identifikation von einer Behörde nur dann verlangt werden, wenn dies in den Verfahrensbestimmungen oder Materiengesetzen ausdrücklich gefordert wird oder auf Grund eines überwiegenden berechtigten Interesses der Behörde notwenig erscheint (§ 3 Abs 2 E-GovG). Eine generelle Vorgabe gibt es dafür nicht, ebenso wenig wann mit einer einfachen Identitätsfeststellung das Auskommen

[9] Erl zur RV 252 BlgNR 22. GP, 15.
[10] Vgl *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 119.
[11] https://finanzonline.bmf.gv.at.
[12] Vgl zB §§ 3 Abs 1 E-GovG, 33 und 35 Abs 3 ZustG.

gefunden werden kann bzw wann die eindeutige Identität festzustellen ist. Die Behörde hat daher im Einzelfall zu entscheiden.[13]

1.3.2 Das Ermittlungsverfahren

Nach erfolgter Verfahrenseinleitung hat die Behörde das Ermittlungsverfahren abzuwickeln. Im Zuge dessen wird der für die Erledigung der Verwaltungssache relevante Sachverhalt ermittelt, wobei die Behörde unter Beachtung der einschlägigen Verwaltungsvorschriften den Gang des Ermittlungsverfahrens relativ frei selbst bestimmen kann (§ 39 Abs 2 AVG). Wurde der Sachverhalt ausreichend erhoben und ist die Sache aus Sicht der Behörde zur Entscheidung reif, so kann sie das Verfahren für geschlossen erklären und zur Erledigung überleiten.

Der Verlauf des Ermittlungsverfahrens kann entweder in einem physischen Akt in Papierform oder auch in einem elektronischen Aktenmanagementsystem (ELAK-System) dokumentiert werden. Auch Aktenvermerke und Niederschriften können beim Einsatz eines ELAK-Systems (ausschließlich) in elektronischer Form verfasst und evident gehalten werden. Die §§ 14 Abs 5 und 16 Abs 2 AVG sehen vor, dass in einem solchen Fall an die Stelle der eigenhändigen Unterschrift des Sachbearbeiters ein elektronisches Verfahren zum Nachweis der Identität und Authentizität treten kann. Da an dieser Stelle nicht der Nachweis der eindeutigen Identität gefordert ist, kann dies auch durch Implementierung eines entsprechenden Berechtigungs- und Rollenkonzepts im ELAK-System erfolgen. Weiters kann auch die Genehmigung einer Erledigung durch eine genehmigungsberechtigte Person auf diese Art und Weise erfolgen (§ 18 Abs 3 AVG).[14]

Werden Verfahrensakten elektronisch erzeugt und genehmigt bzw in einem ELAK-System verwaltet, sind diese gem § 21 Abs 1 E-GovG als das Original zu qualifizieren und in der Form auch anderen Behörden vorzulegen (zB im Zuge eines Instanzenzugs). Die Vorlage hat dabei in einem Standardformat zu erfolgen, welches die Lesbarkeit der Dokumente während der voraussichtlichen Aufbewahrungsdauer nach dem Stand der Technik jeweils bestmöglich gewährleistet (§ 21 Abs 2 E-GovG). Als ein solches Standardformat wird man aktuell jedenfalls PDF/A einstufen dürfen. Für

[13] Vgl *Karning/Kustor*, E-Government in *Bauer/Reimer*, Handbuch Datenschutzrecht, 233.
[14] Erl zur RV 294 BlgNR 23. GP, 13.

die interbehördliche Übermittlung von elektronischen Akten wurde in Österreich das Format EDIAKT II[15] entwickelt, welches auch die Übergabe von Metadaten zu einem Akt, einem Aktenteil und einzelnen Dokumenten ermöglicht. Für die Vorlage elektronischer Akten bei einer anderen Behörde kann auch ein elektronischer Zustelldienst zum Einsatz kommen (§ 21 Abs 3 E-GovG).

1.3.3 Die Genehmigung und Ausfertigung einer Erledigung

Damit eine schriftliche Erledigung als Repräsentation des von der Behörde im Zuge eines Ermittlungsverfahrens gefassten Willens Wirksamkeit entfalten kann, muss diese zuvor von einer befugten Person durch Aufbringung ihrer eigenhändigen Unterschrift genehmigt und im zweiten Schritt dem Betroffenen mittels Zustellung einer Ausfertigung zur Kenntnis gebracht werden (§ 18 AVG). Damit dem Betroffenen sowohl die Identität des Genehmigenden als auch die Authentizität der Ausfertigung (zB des Bescheides) sowie deren Herkunft von einer Behörde erkennbar ist, muss die Ausfertigung folgende Mindestinhalte aufweisen: Bezeichnung der Behörde, Datum der Genehmigung sowie Name als auch Unterschrift der genehmigenden Person (§ 18 Abs 4 AVG). Wird eine Ausfertigung elektronisch erstellt, so kann das Dokument an Stelle der eigenhändigen Unterschrift des Genehmigenden auch mit einer Amtssignatur (§ 19 f E-GovG) versehen werden (vgl Kapitel 12). Dies gilt auch dann, wenn bei der Behörde kein ELAK-System im Einsatz ist, sondern lediglich die einzelnen Dokumente mit Hilfe von zB Textverarbeitungssoftware erstellt werden.

Wird eine Ausfertigung mit einer Amtssignatur versehen, so ist für deren Rechtsgültigkeit keine weitere Voraussetzung (wie zB Ausdruck oder manuelle Unterschrift) notwendig, da bereits das elektronische Dokument die entsprechenden Rechtswirkungen entfaltet. Auch Ausdrucke amtssignierter Dokumente sowie Kopien deren[16] entfalten die gleichen Rechtswirkungen wie das elektronische Original, ohne dass eine gesonderte Unterschrift einer Person notwendig ist. Lediglich dann, wenn ein Dokument zwar elektronisch erstellt jedoch nicht mit einer Amtssignatur versehen wird, muss dieses (seit 1. 1. 2011) als „sonstige Ausfertigung“ iSd § 18 Abs 4 AVG ausgedruckt und von der genehmigungsbefugten Person manuell unterschrieben werden, um Rechtsgültigkeit zu erlangen (vgl § 82a AVG).

[15] Vgl http://reference.e-government.gv.at/EDIAKT.599.0.html, abgerufen am 17. 1. 2012.
[16] Vgl Erl zur RV 290 BlgNR 23. GP, 6.

1.3.4 Die Zustellung

Im letzten Schritt erfolgt die Zustellung der Ausfertigung entweder in physischer oder elektronischer Form, abhängig davon, in welcher Form die Ausfertigung erzeugt wurde, welche Zustellqualität notwendig ist, über welche technischen Einrichtungen die Behörde verfügt und ob der Empfänger bei einem elektronischen Zustelldienst angemeldet ist oder nicht.

Das Zustellgesetz sieht die folgenden Verfahren für die Durchführung einer Zustellung in unterschiedlicher Zustellqualität vor:

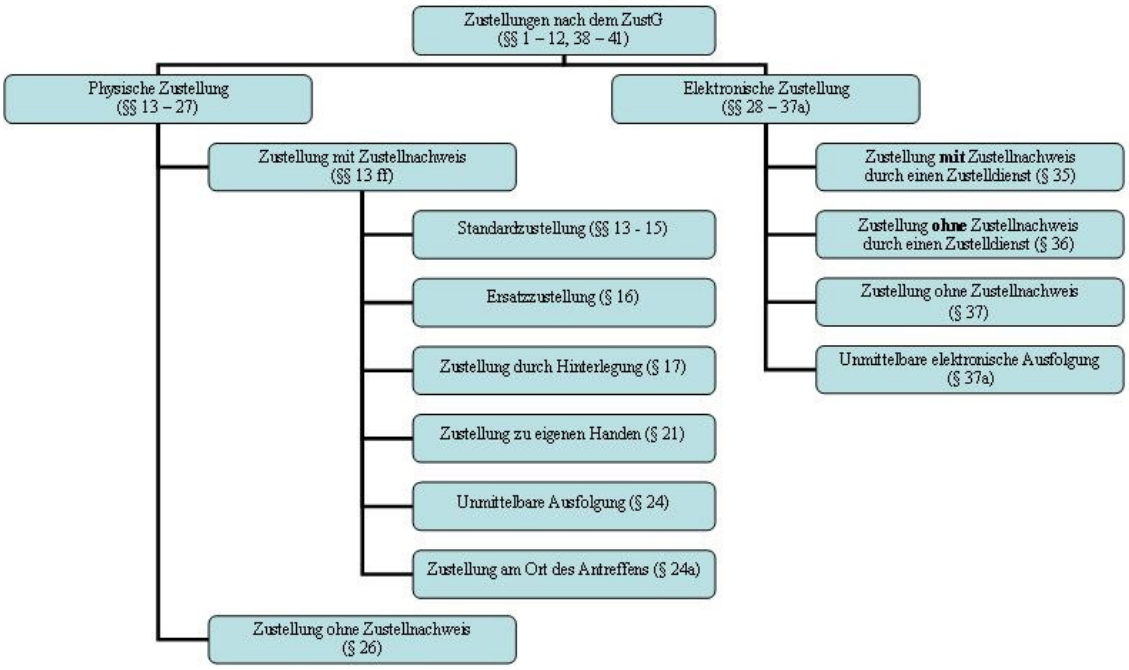

Abbildung 2: Die unterschiedlichen Zustellverfahren

Das ZustG gliedert sich aktuell in 4 Abschnitte, wobei der 1. und 4. Abschnitt allgemeine Regelungen enthalten, welche sowohl für die physische als auch elektronische Zustellung relevant sind. Der 2. Abschnitt enthält die gesamten Regelungen zur physischen Zustellung und der 3. Abschnitt jene über die elektronische Zustellung.
Eine elektronische Zustellung kann grundsätzlich nur über einen gem § 30 ZustG zugelassenen Zustelldienst, über eine „elektronische Zustelladresse“, über ein Zustellsystem der Behörde oder durch unmittelbare elektronische Ausfertigung erfolgen. Ist für die Zustellung ein Zustellnachweis erforderlich, so kommt lediglich die Zustellung durch einen Zustelldienst in Frage, welche aber gleichzeitig auch eine Zustellung zu

eigenen Handen gem § 22 AVG darstellt[17]. Bei einer „elektronischen Zustelladresse“ handelt es sich um eine beliebige elektronische Kontaktadresse (zB E-Mail, Fax, nicht jedoch um ein Postfach bei einem elektronischen Zustelldienst), welche der Empfänger bei Einleitung eines Verfahrens oder im Zuge dessen der Behörde für die Zustellung von Dokumenten bekannt gegeben hat. Welche konkrete Zustellart nun von der Behörde für eine Zustellung gewählt wird, richtet sich nach den konkreten Umständen, den Anforderungen an die Zustellqualität und letztendlich dem Ermessen der Behörde, wobei sich ein solches Ermessen die Einfachheit, Raschheit, Zweckmäßigkeit und die entstehenden Kosten zu berücksichtigen hat (§§ 18 Abs 1 und 22 AVG).

1.3.5 Übersicht über die relevanten Rechtsvorschriften

Zusammengefasst kommen in einem elektronisch geführten oder unterstützten Verwaltungsverfahren neben den Regelungen des AVG gegebenenfalls auch jene des E-Government-Gesetzes (E-GovG) und daraus resultierend die des Signaturgesetzes (SigG) zur Anwendung. Die Anwendbarkeit des SigG ergibt sich daraus, dass einerseits das Konzept der Bürgerkarte gem § 2 Z 10 E-GovG auf einer qualifizierten elektronischen Signatur gem § 2 Z 3a SigG basiert, andererseits aber auch die Amtssignatur gem §§ 19 f E-GovG (zumindest) eine fortgeschrittene elektronische Signatur iSd § 2 Z 3 SigG erfordert. Unabhängig davon sind aber auch die Regelungen des Datenschutzgesetzes (DSG 2000) zu berücksichtigen, wenn personenbezogene Daten automationsunterstützt oder manuell in einer Datei (§ 4 Z 6 DSG) verarbeitet werden. Wie der konkrete Arbeitsablauf innerhalb einer Behörde organisiert ist, ergibt sich auf Grund der innerbehördlichen Organisationshoheit aus der jeweiligen Geschäfts- und Kanzleiordnung, mittels derer jede Behörde autonom ihre Aufbau- und Ablauforganisation regeln kann.

Die folgende Grafik stellt die anwendbaren Gesetze und Regelungen entsprechend dem E-Government-Musterprozess übersichtlich dar, wobei sich die Paragraphenangaben auf das AVG beziehen:

[17] Vgl Erl zur RV 252 BlgNR 22. GP, 19.

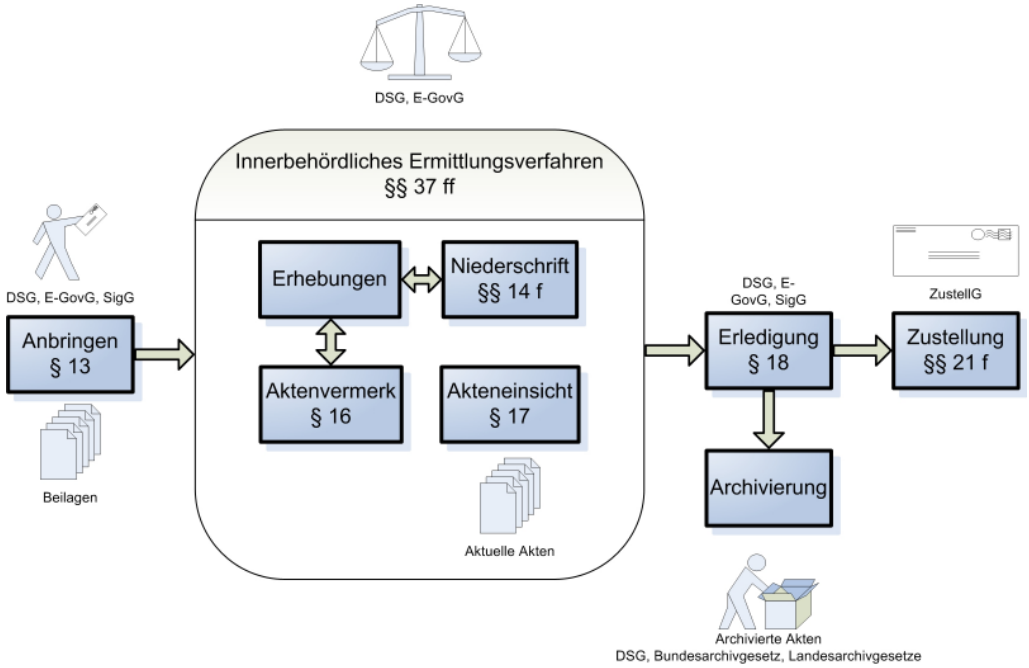

Abbildung 3: Einschlägige Regelungen und Gesetze

Einen in der Literatur kaum behandelten Aspekt von Verwaltungsverfahren stellt die Archivierung von Akten dar. Auch hier regeln in manchen Bereichen gesetzliche Bestimmungen die Handhabung und Aufbewahrungsfrist von Akten abgeschlossener Verfahren. Für Bundesbehörden gilt das Bundesarchivgesetz (BArchG) und auch einige Länder (Oberösterreich, Kärnten, Wien) haben Landesarchivgesetze erlassen. Finden sich keine entsprechenden gesetzlichen Regelungen, ist die Archivierung in der jeweiligen Kanzleiordnung zu regeln.

1.4 Zustellverfügung und Zustellverfahren

Hat eine Behörde eine schriftliche Ausfertigung formgerecht erstellt und möchte sie diese nun dem Rechtsunterworfenen als Empfänger durch Zustellung zur Kenntnis bringen, so ist von der Behörde der Zustellprozess einzuleiten. Der Zustellprozess an sich gliedert sich in zwei voneinander zu unterscheidende Teilaspekte: Die Zustellverfügung (§ 5 ZustG) und der Zustellvorgang (§ 3 ZustG).[18]

1.4.1 Die Zustellverfügung

Die Zustellverfügung bildet den initialen Schritt der Zustellung, in welchem die Behörde a) entscheidet, in welcher Zustellform und –qualität das Dokument zugestellt werden soll und b) abhängig von dieser Entscheidung den Empfänger, an welchen

[18] Vgl VwGH 14. 11. 1955, 2082/52; *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 356, mwN.

das Dokument zugestellt werden soll, in entsprechender Art und Weise möglichst eindeutig bezeichnet.

Somit muss vorerst gem § 22 AVG die Entscheidung getroffen werden, in welcher Zustellqualität die Zustellung erfolgen soll. Dafür stehen 3 Möglichkeiten zur Verfügung: Zu eigenen Handen, mit Zustellnachweis oder ohne Zustellnachweis. Weiters ist über die Zustellform zu entscheiden, also wie und durch welches Organ (§ 3 ZustG) der konkrete Zustellvorgang durchgeführt werden soll. Soll die Zustellung durch einen Zustelldienst (§ 2 Z 7 ZustG) erfolgen, ist weiters zu entscheiden, ob das Dokument physisch oder – sofern die Behörde über eine entsprechende technische Anbindung verfügt und der Empfänger gem § 33 ZustG bei einem elektronischen Zustelldienst angemeldet ist – elektronisch zugestellt werden soll. Sofern keine gesetzliche Regelung eine bestimmte Zustellqualität vorgibt, kann die Behörde nach eigenem Ermessen entsprechend der Wichtigkeit des zuzustellenden Dokuments und unter Rücksichtnahme auf Zweckmäßigkeit, Raschheit, Einfachheit und Kostenersparnis frei wählen.

Weiters ist der Empfänger derart zu individualisieren, dass mit an Sicherheit grenzender Wahrscheinlichkeit auch tatsächlich an jene Person zugestellt wird, welche Adressat der Verwaltungssache ist. Insbesondere bei der physischen Zustellung können sich hier praktische Probleme ergeben, insbesondere dann, wenn zB zwei Personen an ein und derselben Adresse mit dem gleichen Vor- und Nachnamen wohnhaft sind. In einem solchen Fall muss ein zusätzliches Identifikationsmerkmal wie beispielsweise das Geburtsdatum auf dem Dokument angegeben werden, damit die Zustellung auch an den tatsächlich Betroffenen erfolgen kann. Bei der elektronischen Zustellung stellt sich dieses Problem nicht, da hier der Empfänger durch das entsprechende „bereichsspezifische Personenkennzeichen“ (bPK) für den Bereich *Zustellung* eindeutig identifiziert (§ 2 Z 2 E-GovG) wird, wodurch Verwechslungen mit Sicherheit ausgeschlossen werden können (vgl Kapitel 5).
Ist eine elektronische Zustellung seitens der Behörde auf Grund des Vorhandenseins einer entsprechenden technischen Anbindung möglich, so muss vorerst noch geprüft werden, ob der Empfänger überhaupt bei einem elektronischen Zustelldienst angemeldet ist, anderenfalls eine elektronische Zustellung ausscheiden muss. Dies ist durch Abfrage bei einem zentralen Verzeichnisdienst, dem so genannten „Zustell-

kopf“, durchzuführen, der vom Ermittlungs- und Zustelldienst (EuZD) gem § 29 Abs 2 ZustG zu betreiben ist.

Der Behörde stehen somit für die Zustellverfügung zwei Möglichkeiten offen[19]:

- Es wird ausschließlich eine elektronische Zustellung über einen Zustelldienst verfügt. Ist der Empfänger bei keinem elektronischen Zustelldienst angemeldet, so muss die Zustellung erneut verfügt werden, dieses Mal jedoch entweder gem § 37 ZustG oder überhaupt eine physische Zustellung.

- Es wird eine Eventualanordnung für den Fall erlassen, dass der Empfänger bei keinem Zustelldienst angemeldet ist. Es erfolgt somit die Verfügung einer elektronischen Zustellung unter der Bedingung, dass der Empfänger bei einem Zustelldienst angemeldet ist, anderenfalls soll unmittelbar eine physische Zustellung oder Zustellung gem § 37 ZustG erfolgen.

1.4.2 Der Zustellvorgang

Der zweite Schritt ist die konkrete Durchführung der Zustellung, in welchem das zuzustellende Dokument durch das beauftragte Zustellorgan derart in den Machtbereich des Empfängers gebracht wird, dass er von dessen Inhalt mit hoher Wahrscheinlichkeit Kenntnis erlangen kann. Wird die Zustellung entsprechend den Vorschriften des ZustG durchgeführt, treten die Rechtswirkungen der Zustellung auch dann ein, wenn der Empfänger vom Inhalt oder gar von der Existenz des zugestellten Dokuments überhaupt keine Kenntnis erlangte. Der Zustellvorgang wird durch das von der zustellenden Behörde beauftragte Zustellorgan durchgeführt. Kommt dabei ein Zustelldienst als juristische Person des Privatrechts zum Einsatz, so handelt dieser in Form von Public Private Partnership funktionell für die Behörde[20]. Er handelt somit als funktioneller Verwaltungshelfer im Auftrag der Behörde und folglich unselbständig als sozusagen „verlängerter Arm“ der Behörde.[21] Dieser Auffassung folgt auch *Larcher*, obwohl er an anderer Stelle der Auffassung folgt, dass die Anmeldung beim Zustelldienst die Verpflichtung zur Erbringung der Zustellleistung begründe.[22]

---

[19] Vgl Erl zur RV 294 BlgNR 23. GP, 23.
[20] Vgl Erl zur RV 252 BlgNR 22. GP, 4.
[21] *Raschauer*, Allgemeines Verwaltungsrecht, RZ 119 ff. Dies
[22] *Larcher*, Zustellrecht, RZ 540 und 472.

1.4.3 Die Heilung von Zustellmängeln

Sowohl bei der Zustellverfügung als auch bei der Durchführung des Zustellvorgangs können Fehler unterlaufen. Nicht jeder Fehler soll aber sogleich zur Nichtigkeit der Zustellung führen. Deshalb sieht § 7 ZustG die Möglichkeit einer Heilung von Zustellmängeln vor und zwar sowohl für die Zustellverfügung als auch für den Zustellvorgang. Die Zustellung gilt auch bei Vorliegen eines Zustellmangels immer dann als rechtlich wirksam vorgenommen, wenn das Dokument dem formell bezeichneten Empfänger tatsächlich zukommt, also in dessen Verfügungsgewalt zugeht. Eine anderweitige Kenntnisnahme des Inhalts reicht dafür jedoch nicht aus.[23]

1.5 Die rechtliche Stellung des Zustellorgans

Die Behörde kann Zustellungen entweder selbst durchführen, indem sie Bedienstete oder einen zugelassenen Zustelldienst damit beauftragt, aber sie kann auch selbst einen Zustelldienst betreiben, der jedoch gleichermaßen den Regelungen des ZustG entsprechen muss und einer Zulassung bedarf[24].[25] Unter Zustelldienst versteht § 2 Z 7 ZustG die Österreichische Post AG oder einen anderen Universaldienstbetreiber gem § 6 Postmarktgesetz (PMG)[26] für die physische Zustellung sowie einen gem § 30 ZustG zugelassenen elektronischen Zustelldienst für den Anwendungsbereich des 3. Abschnitts (außer §§ 37 und 37a ZustG).

Anmerkung: Mit 31. 12. 2010 trat das Postgesetz 1997, auf welches § 2 Z 7 ZustG in seiner gültigen Fassung noch immer[27] verweist, außer Kraft, dafür traten die entsprechenden Regelungen des Postmarktgesetzes (PMG) mit 1. 1. 2011 in Kraft. Die Anpassung dieses Verweises im ZustG wurde offenbar übersehen.

Die rechtliche Stellung des Zustellorgans wird in § 4 ZustG geregelt: Dieser sieht vor, dass das Zustellorgan, welches von der Behörde in der Zustellverfügung mit der Durchführung des Zustellvorgangs betraut wurde, hinsichtlich der Wahrung der Ge-

---

[23] Vgl *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 356 f; *Feil*, Zustellrecht, 32 f; *Raschauer/Sander/Wessely*, Österreichisches Zustellrecht, 51 ff.

[24] Dies ergibt sich aus der Tatsache, dass die Unterscheidung zwischen behördlichen und privaten Zustelldiensten mit der Novelle des ZustG BGBl I 5/2008 aufgegeben wurde und beide Arten folglich gleichermaßen zu behandeln sein werden (vgl Erl zur RV BlgNR 294 23. GP, 3).

[25] Die speziellen gesetzlichen Voraussetzungen für die Zustellung durch Bedienstete der Behörde oder durch Gemeindeorgane seien an dieser Stelle nicht erläutert.

[26] Postmarktgesetz (BGBl I Nr 123/2009 idF 111/2010).

[27] Stand: 12. 6. 2011.

setzmäßigkeit als *Organ der Behörde* handelt. Daraus sowie auch schon aus § 1 ZustG („in Vollziehung der Gesetze“) ergibt sich, dass nicht nur der Zustellverfügung sondern auch dem Zustellvorgang hoheitlicher Charakter beizumessen ist und es sich dabei nicht um *bloßes* Verwaltungshandeln – geschweige denn Privatwirtschaftsverwaltung – handelt. Auch bei der Durchführung des Zustellvorgangs handelt der Zustelldienst mit Imperium als *funktionell* tätiges Organ der Behörde, wobei die Zustellbehörde jene Behörde ist, in deren Namen zugestellt werden soll. Unter *Organen im bloß funktionellen Sinn* versteht man solche Organe einer juristischen Person, welche zwar keine Organe der Rechtsperson im organisatorischen Sinn sind, deren Handeln jedoch der entsprechenden juristischen Person (zB Behörde) zugerechnet wird.[28] § 4 ZustG stellt ausdrücklich klar, dass der Zustelldienstbetreiber als juristische Person bezüglich des Zustellvorgangs in Form eines (bloß) funktionellen Organs[29] der jeweiligen Behörde und somit gewisser Maßen als deren „verlängerter Arm“ auftritt. Da der Zustelldienst selbst keinen vollständigen Hoheitsakt in eigenem Ermessen setzen kann, sondern bloß mit einem unselbständigen Teilakt – der Durchführung des Zustellvorgangs – betraut wird, handelt es sich dabei um keine Beleihung, sondern der Zustelldienst tritt als lediglich unselbständiger Verwaltungshelfer auf. Die Verwaltungshelfereigenschaft ergibt sich aus dem Auftrag der Behörde, wobei dies ein Vertrag oder ein Bescheid sein kann.[30]

Aus dieser Organstellung folgt, dass Schäden, welche ein Zustelldienst im Zuge eines Zustellvorgangs einem Dritten schuldhaft verursacht, gemäß der Regelungen des Amtshaftungsgesetzes (AHG) vom Rechtsträger jener Behörde, für welche die Zustellung erfolgte, zu ersetzen sind (§ 1 AHG). Dies gilt unabhängig davon, ob der Schaden aus der Verletzung des ZustG oder einer sonstigen gesetzlichen Regelung bzw aus einem Tun oder Unterlassen resultiert. Der Zustelldienst selbst haftet dem Geschädigten zwar nicht, jedoch kann sich der Rechtsträger der belangten Behörde beim Zustelldienst schadlos halten, wenn dieser den Schaden vorsätzlich oder grob fahrlässig verursacht hat (§ 3 AHG). Für den Bereich der physischen Zustellung stellt dies § 17 PMG nochmals ausdrücklich klar, für den Bereich der elektronischen Zustellung lässt sich dieser Umstand lediglich aus § 4 ZustG ableiten, da ein Zustell-

[28] Vgl *Raschauer*, Allgemeines Verwaltungsrecht, RZ 109.
[29] Die Behörde könnte einen Zustelldienst auch selbst betreiben, wodurch dieser nicht bloß funktionell sondern auch organisatorisch als Organ dieser Behörde anzusehen wäre.
[30] *Raschauer*, Allgemeines Verwaltungsrecht, RZ 119 f.

dienst als funktionelles Organ der zustellenden Behörde handelt und daher die Regelungen des AHG für den Ersatz von Schäden anzuwenden sind.[31]

1.6 Die Zulassung als elektronischer Zustelldienst

Um als elektronischer Zustelldienst am Markt tätig sein und die Erbringung von Zustellleistungen anbieten zu dürfen, bedarf es einer vorherigen Zulassung gem § 30 ZustG durch den Bundeskanzler. Die Zulassung ist beim Bundeskanzler zu beantragen und wird per Bescheid zugesprochen. Gegebenenfalls können auch Auflagen erteilt werden. Die zugelassenen Zustelldienste einschließlich der erteilten Auflagen und vorgeschriebenen Bedingungen sind im Internet[32] zu veröffentlichen (§ 30 Abs 3). Tritt der Fall ein, dass eine Zulassungsvoraussetzung wegfällt oder ein ursprünglicher Mangel nachträglich hervorkommt, so ist zuerst die Behebung dieses Mangels unter Setzung einer angemessenen Frist anzuordnen. Wird dieser Anordnung nicht oder nicht innerhalb der festgesetzten Frist entsprochen, so ist die Zulassung per Bescheid zu widerrufen (Abs 4).[33] Eine Zulassung kann einem Zustelldienst jedoch nur dann entzogen werden, wenn die Leistungen des § 29 Abs 1 ZustG mangelhaft erbracht werden, nicht jedoch in jenem Fall, in welchem dies lediglich die Leistungen des Abs 2 betrifft. Solche Mängel berühren ausschließlich das Vertragsverhältnis zwischen dem Bundeskanzler und dem EuZD gem § 32 Abs 1 ZustG, wodurch sich der BK bei mangelhafter Erfüllung der vertraglichen Pflichten durch den EuZD lediglich zivilrechtlicher Instrumente bedienen kann (zB Gewährleistung, außerordentliche Kündigung, etc).[34] Nichtsdestotrotz muss ein Widerruf der Zulassung des EuZD gem § 30 Abs 4 ZustG auf Grund der mangelhaften Erbringung der Zustellleistung auch dazu führen, dass dieser die Leistungen des § 29 Abs 2 ZustG ebenfalls nicht mehr erbringen darf und dass die Pflicht zur Erbringung der Ermittlungs- und Verrechnungsleistung unmittelbar wieder den Übergangszustelldienst gem § 32 Abs 2 ZustG – wenn auch nur interimsmäßig – trifft. Auch wenn der diesbezügliche zivilrechtliche Vertrag zwischen BK und EuZD auf Grund von mangelhafter Leistungserbringung aufgelöst wird, müssen diese Leistungen wiederum vom Übergangszustelldienst erbracht werden (vgl Kapitel 9.7).

---

[31] Vgl *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 358; *Feil*, Zustellwesen, 24 f.
[32] http://www.bka.gv.at/DesktopDefault.aspx?TabID=4633, abgerufen am 17. 1. 2012.
[33] Vgl *Larcher*, Zustellrecht, RZ 467.
[34] Vgl Erl zur RV 294 BlgNR 23. GP, 22.

Weiters unterliegen die zugelassenen Zustelldienste der laufenden Aufsicht durch den Bundeskanzler (§ 31 ZustG), der diese Aufsicht dahingehend auszuüben hat, dass die Zustelldienste die einschlägigen Gesetze und Verordnungen einhalten und die sich daraus ergebenden Aufgaben ordnungsgemäß erfüllen. Die für die Durchführung der Aufsicht notwendigen Auskünfte sind dem Bundeskanzler unverzüglich, jedoch längstens binnen 2 Wochen zu erteilen. Unter solchen „Auskünften" verstehen die EB eine detaillierte Systembeschreibung, „aus welcher hervorgeht, ob alle zum zuverlässigen und leistungsfähigen Betrieb erforderlichen organisatorischen und technischen Maßnahmen ergriffen wurden, und in der die zugrunde liegende Infrastruktur, die verwendeten Systemkomponenten sowie die angewendeten Sicherheits-, Betriebs- und Notfallkonzepte erläutert werden"[35]. Ändern sich bei einem Zustelldienst Umstände, welche für die Erteilung einer Zulassung relevant sind bzw waren oder welche sich auf die ordnungsgemäße Erbringung der Leistungen auswirken, so muss dies der Zustelldienst dem Bundeskanzler unverzüglich bekannt geben.

2. Ablauf und Akteure der elektronischen Zustellung

Der gesamte Vorgang der elektronischen Zustellung und das dafür gesetzlich zu implementierende System stellt ein „verteiltes System" im technischen Sinne dar, welches eine Vielzahl von Computersystemen verschiedenster Personen und Organisationen miteinander vernetzt und welches eine fehlerfreie und zuverlässige Kommunikation gewährleisten muss. Aus diesem Grund kann das gesamte System, in welchem die vom ZustG geforderten Leistungen (Zustellleistung, Ermittlungsleistung und Verrechnungsleistung) von verschiedenen Akteuren zu erbringen sind, konsequenter Weise als „Zustellsystem" bezeichnet werden, auch wenn es sich dabei nicht um einen Rechtsbegriff handelt. In diesem gesamten Zustellsystem erbringen oder konsumieren verschiedene Akteure unterschiedliche „Leistungen", wobei sich der Inhalt dieser Leistungen und die Akteure direkt aus dem Zustellgesetz ergeben.

Das Zustellgesetz definiert in § 29 ZustG die drei Hauptleistungen, welche bei jedem einzelnen Zustellvorgang ausgeführt werden müssen:

- Die **Ermittlungsleistung** (§ 29 Abs 2 Z 2 ZustG) vom Ermittlungs- und Zustelldienst („Zustellkopf"): Im ersten Schritt muss die Behörde beim Zustellkopf

[35] Erl zur RV BlgNR 294 23. GP, 22.

– einem zentralen Verzeichnisdienst zu Verwaltung aller Personen, welche bei irgendeinem elektronischen Zustelldienst angemeldet sind – abfragen, ob der potentielle Empfänger bei (irgendeinem) Zustelldienst angemeldet ist und ggf bei welchem.

- Die **Zustellleistung** (§ 29 Abs 1 ZustG) von einem jener Zustelldienste, bei welchen der Empfänger angemeldet ist: Die Behörde übergibt dafür das zuzustellende Dokument an den Zustelldienst zur Durchführung der Zustellung. Der Empfänger bestätigt die Abholung und deren Zeitpunkt mit seiner digitalen Unterschrift, welche der Behörde im Anschluss zusammen mit weiteren Daten als Zustellnachweis übermittelt wird.

- Die **Verrechnungsleistung** (§ 29 Abs 2 Z 3 ZustG) durch den Ermittlungs- und Zustelldienst: Jeder Zustelldienst übermittelt in periodischen Abständen die Daten über durchgeführte Zustellungen an den Zustellkopf, welcher die Daten aller Zustelldienste getrennt nach Behörden entsprechend kumuliert und den jeweiligen Behörden, für welche Zustellungen durchgeführt wurden, die jeweiligen Entgelte in Rechnung stellt. Im Anschluss leitet der Zustellkopf die kassierten Entgelte entsprechend an die jeweiligen Zustelldienste weiter.

Die folgenden Leistungen sind zwar im Gesetz nicht explizit genannt, stellen aber dennoch Leistungen dar, die für ein reibungsloses Funktionieren des gesamten Zustellsystems notwendig sind. Das Charakteristikum dieser Leistungen ist, dass sie unabhängig von einer konkreten Zustellverfügung laufend zu erbringen sind. Sie stellen somit allgemeine Leistungen dar, die nicht als hoheitliche Tätigkeit gem § 4 ZustG einzustufen sind, da sie sich auf keinen konkreten Zustellvorgang beziehen.

- Die **„Zentrale Speicherleistung“** (§ 29 Abs 2 Z 1 ZustG) stellt zwar an sich keine separat zu betrachtende Leistung dar, jedoch dient sie als Basis der für das gesamte Zustellsystem zentralen Ermittlungs- und Verrechnungsleistung und verbindet diese beiden Leistungen somit zu einer untrennbaren Einheit. Sie umfasst die Führung eines für das gesamte Zustellsystem zentralen Verzeichnisdienstes, in welchem die Kundendaten aller bei einem Zustelldienst angemeldeten Kunden zentral verwaltet werden und bildet daher die Basis für

die Erbringung der Ermittlungsleistung. Auch die Daten für die Erbringung der Verrechnungsleistung werden so verwaltet.

- Die **„Aktualisierungsleistung“** (§ 29 Abs 1 Z 1 ZustG) ist von jedem Zustelldienst verpflichtend auszuführen, wenn sich bei diesem ein neuer Kunde anmeldet, ein bestehender Kunde seine Daten ändert oder ein Kunde sich abmeldet. Diese Information muss unverzüglich dem Zustellkopf übermittelt werden, der sie in seinen Verzeichnisdienst übernehmen muss.[36]

2.1 Das Verfahren der elektronischen Zustellung

Damit von einer Behörde eine elektronische Zustellung von Dokumenten mit Zustellnachweis an einen bestimmten Empfänger verfügt werden kann, muss dieser bei einem beliebigen zugelassenen Zustelldienst angemeldet sein. Ist der Empfänger nicht bei einem elektronischen Zustelldienst angemeldet, bleibt der Behörde nur die Möglichkeit, eine physische Zustellung zu verfügen. Die folgende Grafik beschreibt den Ablauf einer elektronischen Zustellung unter Einsatz eines Zustelldienstes:

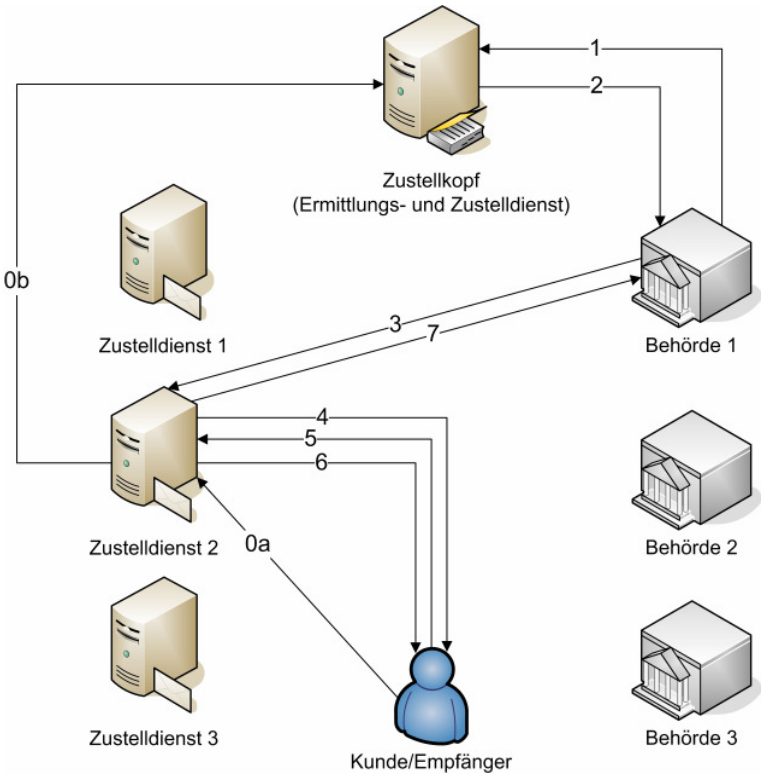

Abbildung 4: Ablauf eines elektronischen Zustellvorgangs

[36] Zwar finden sich weder der Terminus der *„Zentralen Speicherleistung“* noch jener der *„Aktualisierungsleistung“* im Gesetz oder der Literatur, jedoch werden diese in weiterer Folge auf Grund ihres selbsterklärenden und deskriptiven Charakters zur einheitlichen Bezeichnung der in § 29 Abs 2 Z 1 und Abs 1 Z 1 ZustG aufgelisteten Leistungen verwendet.

Schritt 0a: Anmeldung durch den Kunden (§ 33 ZustG)

Damit sich einer Behörde überhaupt die Möglichkeit einer elektronischen Zustellung bietet, muss sich der potentielle Empfänger zuvor bei einem zugelassenen Zustelldienst seiner Wahl gem § 33 ZustG angemeldet haben (vgl Kapitel 4). Dafür hat er das vom Zustelldienst gem § 33 Abs 1 2. Satz zur Verfügung gestellte Verfahren zur Anmeldung auszuführen. Im Zuge der Anmeldung müssen auch bestimmte Daten zur Person bekannt gegeben werden und die Anmeldedaten unter Verwendung der Bürgerkarte digital signiert werden. Nach erfolgter Anmeldung ist diese Person als „Kunde" gem § 2 Z 9 ZustG zu qualifizieren. Eine solche Anmeldung muss nur einmal ausgeführt werden und ist nicht von einer Zustellverfügung einer Behörde gem § 5 ZustG abhängig. Schritt 0a kann auch die Änderung von Kundendaten oder die Abmeldung vom Zustelldienst darstellen.

Schritt 0b: Aktualisierung des Zustellkopfs (§ 29 Abs 1 Z 1 ZustG)

Hat sich ein Kunde bei einem Zustelldienst angemeldet, Änderungen in seinen Kundendaten bekannt gegeben oder sich beim Zustelldienst abgemeldet, so sind solche Informationen vom betroffenen Zustelldienst „unverzüglich" dem EuZD bekannt zu geben. Schritt 0b wird stets nur in unmittelbarem Zusammenhang mit Schritt 0a ausgeführt und bildet die eingangs beschriebene *Aktualisierungsleistung*.

Schritt 1: Adressierbarkeitsabfrage beim Zustellkopf (§ 34 Abs 1 Satz 1 ZustG)

Möchte nun eine Behörde ein Dokument in elektronischer Form an einen Empfänger zustellen und verfügt sie über die technische Anbindung an das elektronische Zustellsystem, muss sie dafür nun im ersten Schritt den EuZD mit der Durchführung der *Ermittlungsleistung* beauftragen. Dafür setzt sie bei diesem unter Angabe bestimmter zulässiger Suchparameter[37] eine Anfrage ab, ob der Empfänger bei einem der zugelassenen Zustelldienste angemeldet ist und gegebenenfalls bei welchem. Diese Abfrage wird als „Adressierbarkeitsabfrage" bezeichnet, da mit ihr ermittelt werden soll, ob ein designierter Empfänger elektronisch adressierbar ist, also bei einem elektronischen Zustelldienst angemeldet ist.

[37] §§ 34 Abs 2 IS iVm 33 Abs 1 Z 1 – 5 ZustG.

Schritt 2: Adressierbarkeitsantwort vom Zustellkopf (§ 34 Abs 1 Satz 2 ZustG)

Der Zustellkopf retourniert daraufhin eine entsprechende Antwort, nämlich dass der Empfänger entweder bei keinem Zustelldienst angemeldet ist (bzw für den aktuellen Zeitpunkt einen Zustellausschluss gem § 33 Abs 2 lS verfügt hat), oder im positiven Fall die notwendigen Daten zur Übergabe des Dokuments an den Zustelldienst und dessen Zustellung an den Empfänger. Dies sind die Internetadresse des Zustelldienstes, die vom Empfänger akzeptierten Dateiformate sowie gegebenenfalls vom Empfänger hinterlegte Angaben zur inhaltlichen Verschlüsselung.[38] Zusätzlich wird vom Zustellkopf ein Verrechnungstoken (vgl Kaptitel 7.6) generiert, welcher das bPK für den Verwaltungsbereich „Zustellung“ bzw die Stammzahl des Empfängers beinhaltet und mit dem öffentlichen Schlüssel des jeweiligen Zustelldienstes verschlüsselt wird.[39] Stammzahl und bPK werden vom Gesetz nicht explizit als zu übermittelnde Daten angeführt, was darauf zurückzuführen sein dürfte, dass die anfragende Behörde entweder ohnedies über diese Information verfügt oder den Inhalt des Tokens auf Grund der Verschlüsselung ohnedies nicht interpretieren kann.

Schritt 3: Übermittlung an den Zustelldienst (§ 34 Abs 1 Satz 3 ZustG)

Die Behörde hat nun entsprechend der gesetzlichen Vorgaben jenen Zustelldienst auszuwählen, welcher den Zustellvorgang durchführen soll. Zu bevorzugen sind in erster Linie jene Zustelldienste, bei welchen der Kunde Daten zur inhaltlichen Verschlüsselung (§ 33 Abs 1 Z 7 ZustG) hinterlegt hat (§ 34 Abs 3 ZustG). Hat ein Kunde bei keinem Zustelldienst Verschlüsselungsdaten oder solche bei mehreren Zustelldiensten hinterlegt, ist von der Behörde auf Grund der Kriterien der Zweckmäßigkeit, Raschheit, Einfachheit und Kostenersparnis (vgl § 18 AVG) der am geeignetsten erscheinende Zustelldienst zu wählen. Da für die Erbringung der Zustellleistung jedoch alle Zustelldienste dasselbe Entgelt erhalten, muss die Auswahl hier dem Zufall überlassen werden. Die Behörde übergibt nun das zuzustellende Dokument zusammen mit dem vom Zustellkopf erhaltenen Verrechnungstoken an den gewählten Zustelldienst.

[38] § 34 Abs 1 2. Satz ZustG.
[39] *Tauber/Rössler*, ZUSEKOPF, 26.

Schritt 4: Verständigung des Empfängers (§ 35 Abs 1 ZustG)

Langt das zuzustellende Dokument beim Zustelldienst ein, so muss der Zustelldienst den entsprechenden Empfänger über diesen Umstand informieren. Dafür ist an die im Zuge der Anmeldung gem § 33 ZustG bekannt gegebene elektronische Adresse (Abs 1 Z 4) eine entsprechende Mitteilung zu versenden, dass ein Dokument zur Abholung bereitliegt (also elektronisch für ihn beim Zustelldienst zur Abholung hinterlegt wurde). Gegebenenfalls muss auch eine zweite Verständigung an diese elektronische Adresse erfolgen und eine dritte in physischer Form an eine dem Zustelldienst bekannt gegebene Abgabestelle (§ 2 Z 4 ZustG). Die detaillierten Regelungen bezüglich der Fristen und den Eintritt der Zustellwirkung finden sich in den §§ 35 f, je nachdem, ob zu eigenen Handen (§ 35) oder ohne Zustellnachweis (§ 36) zugestellt werden soll. Zu beachten ist in diesem Zusammenhang, dass die Zustellwirkung auch dann eintreten kann, wenn der Empfänger das bereitliegende Dokument nicht abholt und somit von dessen Inhalt gar keine Kenntnis hatte!

Schritt 5: Authentifizierung durch den Empfänger (§ 35 Abs 3 ZustG)

Nachdem der Empfänger von der Bereithaltung eines Dokuments informiert wurde, baut der Empfänger eine elektronische Verbindung zum entsprechenden Zustelldienst auf (zB durch Aufruf der Internetseite des Zustelldienstes). Bevor dem Empfänger jedoch bereitliegende Dokumente angezeigt werden und diesem somit Informationen über die zuzustellenden Dokumente hinsichtlich Absender, Inhalt, etc preisgegeben werden, muss sich der Empfänger gegenüber dem Zustelldienst unter Verwendung seiner Bürgerkarte gem § 2 Z 10 E-GovG authentifizieren (§ 35 Abs 3 Satz 3 ZustG).[40] Dies erfolgt dadurch, dass der Bürgerkartenumgebung (BKU) des Empfängers ein bestimmter Datensatz (der „AuthBlock“) zur digitalen Signierung übergeben wird. Nachdem der Empfänger diesen AuthBlock signiert hat, führt der Zustelldienst die Signaturprüfung durch. Ist diese erfolgreich, konnte die Identität des Empfängers und Authentizität der Zugangsberechtigung erfolgreich nachgewiesen werden und der Zugang zu den Dokumenten wird freigegeben.

[40] Analog zur physischen Zustellung kann der Empfänger auch Zustellungsbevollmächtigte gem § 9 ZustG beauftragen, die stellvertretend für den Empfänger Dokumente in Empfang nehmen dürfen. Da sich diese Regelungen bezüglich Zustellungsbevollmächtigten im allgemeinen 1. Abschnitt des Zustellgesetzes befinden, kommen diese sowohl bei der physischen als auch elektronisches Zustellung zur Anwendung. Dafür ist es jedoch notwendig, dass die Stellvertretungsbefugnis gem § 5 E-GovG in der Bürgerkarte eingetragen ist.

Dieser dem Empfänger vorzulegende AuthBlock muss die Daten der aus der Bürgerkarte auszulesenden Personenbindung (Vorname, Nachname, Geburtsdatum oder Bezeichnung der juristischen Person), Datum und Uhrzeit jenes Zeitpunktes, zu welchem der zu signierende Text an den Empfänger übermittelt wurde, und die URI des Zustelldienstes beinhalten. Dadurch bleibt einerseits augenscheinlich erkennbar, welche eindeutig identifizierte Person diesen Text signiert hat und andererseits wird dadurch festgelegt, zu welchem Zeitpunkt alle beim Zustelldienst bereitliegenden Dokumente als durch den Empfänger abgeholt gelten. Aus Gründen der Usability muss nicht die Abholung eines jeden einzelnen Dokuments digital signiert werden, sondern mit dem Login gelten alle bereitliegenden Dokumente als zugestellt.[41] Der signierte AuthBlock bildet in der Folge den Zustellnachweis gem § 35 Abs 3 lS ZustG.

Die Daten zur Person des Empfängers in diesem Text sind notwendig, dass zu einem späteren Zeitpunkt die entsprechenden Daten zur Signaturprüfung aufgefunden werden können. Auch das Datum ist hierfür wichtig, da das Zertifikat des Empfängers nur für einen begrenzten Zeitraum Gültigkeit besitzt. Liegt der Zeitpunkt der Signaturerstellung bereits längere Zeit zurück, so kann dadurch sichergestellt werden, dass das zum damaligen Zeitpunkt gültige Zertifikat (und der damit verbundene öffentliche Schlüssel des Empfängers) identifiziert und damit die Signaturprüfung durchgeführt werden kann. Üblicherweise zeigt die BKU dem Empfänger die Aufforderung zur Durchführung der digitalen Signatur wie in Abbildung 5 dargestellt an:

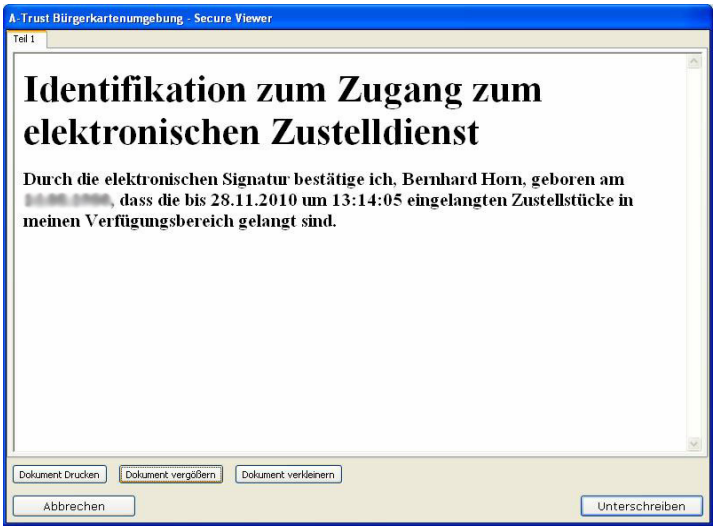

Abbildung 5: Authentifizierung beim Zustelldienst und Signierung eines Zustellnachweises

[41] *Rössler/Tauber/Reichstädter*, ZUSEMSG, 24.

Es besteht zwar keine explizite gesetzliche Verpflichtung, den Empfänger in dem zu unterschreibenden Text auf die Rechtswirkungen der Abholung hinzuweisen, jedoch ist dies im Sinne einer Good Governance und Bürgerorientiertheit empfehlenswert. Gelegentlich findet sich als zu signierender Text die Klausel: *„Mit meiner elektronischen Signatur beantrage ich, Bernhard Horn, geboren am XX. XX. XXXX, den Zugang zur gesicherten Anwendung. Datum und Uhrzeit: 12. 6. 2011, 12:00:00."*

Das Zustellgesetz erlaubt aber auch den Einsatz automatisiert ausgelöster Signaturverfahren (§ 35 Abs 3 Satz 3 ZustG). Vorrausetzung dafür ist, dass diese sowohl an die Verwendung einer sicheren Technik gebunden ist und dies auf Grund einer „besonderen Vereinbarung" mit dem Zustelldienst erfolgt. Dies bedeutet, dass der Zustelldienst eine solche Möglichkeit nicht anbieten muss, falls er dies aber tut, kann der Kunde diese Möglichkeit mittels einer zivilrechtlichen Vereinbarung mit dem Zustelldienst in Anspruch nehmen. Die technische Spezifikation für diese Methode der Abholung findet sich in ZUSEMAIL[42] am Referenzserver.

Schritt 6: Abholung durch den Empfänger

Dieser Schritt erfolgt in engem Zusammenhang mit Schritt 5. Hat der Empfänger den ihm zur Signatur vorgelegten Text digital signiert und sich dadurch erfolgreich gegenüber dem Zustelldienst authentifiziert, werden ihm sämtliche bereitliegenden Dokumente angezeigt und er kann diese öffnen[43] oder downloaden. Welche konkreten Informationen dem Empfänger über die bereitgehaltenen Dokumente anzuzeigen sind, erschließt sich aus keiner gesetzlichen Regelung, jedoch erscheinen zumindest folgende Angaben als sinnvoll:

- Absender
- Betreff
- Begleittext
- Zustellzeitpunkt
- Zustellqualität

[42] *Posch/Rössler*, Abholung von Zustellung über E-Mail-Clients.
[43] Korrekter Weise muss festgehalten werden, dass auch das Öffnen genau genommen einen Download darstellt.

  - Zustellung mit Zustellnachweis (§ 35 ZustG)
  - Zustellung ohne Zustellnachweis (§ 36 ZustG)
  - Zustellung im Auftrag Privater (§ 29 Abs 3 ZustG, vgl ZUSEPRIV)
- Ende der Bereithaltefrist (§ 35 Abs 4 ZustG)

Es empfiehlt sich, an dieser Stelle dem Empfänger nicht nur das Öffnen oder Downloaden der bereitliegenden Dokumente zu ermöglichen, sondern entsprechend dem gesetzlichen Rahmen und gegebenenfalls auf Grund privatrechtlicher Vereinbarung weitere Funktionen zur Verfügung zu stellen. Dies könnten beispielsweise die Weiterleitung der Dokumente an eine herkömmliche E-Mail-Adresse oder die Anforderung von Ausdrucken oder Kopien des Dokuments in physischer Form gem § 29 Abs 1 Z 10 ZustG sein.

Zu beachten ist weiters, dass es dem Empfänger nicht möglich sein darf, entsprechend den Regelungen des Zustellgesetzes bereitliegende Dokumente zu löschen. Diese müssen gem § 35 Abs 4 Satz 2 ZustG nämlich jedenfalls – da es sich bei den Regelungen des ZustG um zwingendes Recht handelt[44] – 2 Wochen nach Abholung weiterhin verfügbar gehalten werden und sind danach automatisch zu löschen. Eine darüber hinausgehende Speicherung ist auf Grund einer eigenständigen zivilrechtlichen Vereinbarung mit dem Zustelldienst zwar gesetzlich möglich, jedoch unterliegt eine solche Bereithaltung als Hosting-Dienstleistung gem § 16 ECG nicht mehr den Regelungen des Zustellgesetzes sondern jenen des ECG und des allgemeinen Zivilrechts (vgl Kapitel 11.3.1). In einem solchen Fall muss eine Löschung selbstverständlich möglich sein (§ 6 Abs 1 Z 5 DSG).

Schritt 7: Übermittlung des Zustellnachweises (§ 35 Abs 3 IS ZustG)

Im letzten Schritt muss der Zustelldienst nun all jenen Behörden den Zustellnachweis übermitteln, deren Dokumente beim Zustelldienst für den Empfänger bereitgehalten wurden und welche dieser nun im Zuge des in Schritt 5 durchgeführten Signaturvorgangs abgeholt hat. Dieser Zustellnachweis muss die Daten der gem § 35 Abs 1 und 2 durchgeführten Verständigungen sowohl an der elektronischen als auch physischen Adresse beinhalten, sowie den vom Empfänger im Zuge der Authentifikation

[44] Erl zur RV 252 BlgNR 22. GP, 14.

beim Zustelldienst digital signierten Text (Authblock). Aus diesem Authblock gehen wie in Schritt 5 beschrieben sowohl die eindeutige Identität des Empfängers als auch die Verständigungs- und Zustellzeitpunkte hervor. Da dieser Authblock vom Empfänger und der gesamte Zustellnachweis vom Zustelldienst digital signiert wurden, kann die zustellende Behörde jederzeit unter Verwendung des jeweiligen öffentlichen Schlüssels die Authentizität des Zustellnachweises prüfen.

2.2 Der Eintritt der Zustellwirkung

Wie bereits in Kapitel 1.2 ausgeführt, sollen die gesetzlichen Regelungen des ZustG nach Möglichkeit erreichen, dass der Inhalt eines zuzustellenden Dokuments dem Empfänger in aller Regel zur Kenntnis gelangt. Die Zustellwirkung tritt jedenfalls mit Abholung durch den Empfänger ein, sofern sie auf Grund einer der Regelungen des ZustG nicht schon früher eingetreten ist (§ 35 Abs 5 ZustG). Unter der Voraussetzung, dass die Zustellregelungen eingehalten wurden, treten die mit einer solchen Zustellung verbundenen Rechtswirkungen auch dann ein, wenn der Empfänger – aus welchen Gründen auch immer – vom Inhalt oder der Existenz der zuzustellenden Dokumente keine Kenntnis erlangte. Abhängig davon, ob mit oder ohne Zustellnachweis zuzustellen ist, tritt die Zustellwirkung unter verschiedenen Voraussetzungen ein.

Liegt nun ein Dokument für einen Empfänger beim Zustelldienst bereit, so muss der Zustelldienst an die bzw alle vom Empfänger bekannt gegebene(n) elektronische(n) Adresse(n) eine Verständigung über das Bereitliegen senden. Eine solche Verständigung muss die in § 35 Abs 1 ZustG vorgesehenen Inhalte aufweisen und entsprechend der Zustellformularverordnung 1982[45] gestaltet sein, wobei sich in der Anlage zur VO detaillierte (normative) Musterformulare[46] befinden. Verstreichen 48 Stunden ohne Abholung, ist auf dieselbe Weise erneut eine elektronische Verständigung zu versenden. Erfolgte nach weiteren 24 Stunden noch immer keine Abholung, ist bei einer Zustellung mit Zustellnachweis der Empfänger postalisch an der angegebenen Abgabestellte zu verständigen, sofern eine solche angegeben wurde. Eine postali-

[45] BGBl 600/1982 idF BGBl II 152/2008.

[46] Relevant für die elektronische Zustellung sind die Formulare 7 – 9. „*Hat der Empfänger dem Zustelldienst eine Abgabestelle bekannt gegeben, so ist bei der Zustellung mit Zustellnachweis für die elektronischen Verständigungen das Formular 8 zu verwenden; in den übrigen Fällen ist für die elektronischen Verständigungen das Formular 7 zu verwenden. Für die postalischen Verständigungen ist das Formular 9 zu verwenden*“ (§ 3a Abs 2 ZustFormV).

sche Verständigung bei einer Zustellung ohne Zustellnachweis erfolgt nicht (§ 36 ZustG). Abhängig davon, ob nun eine Zustellung mit oder ohne Zustellnachweis erfolgt und ob der Empfänger eine (physische) Abgabestellte für eine postalische Verständigung angegeben hat, tritt die Zustellwirkung bei Nichtabholung zu unterschiedlichen Zeitpunkten ein. Diese Regelungen sind bedauerlicherweise sehr kasuistisch und schwer verständlich, insbesondere in § 36 ZustG wird zur Vermeidung textlicher Redundanzen mit umfassender Verweistechnik gearbeitet. Bezüglich der Regelungen über den Eintritt der Zustellwirkung wird auf die §§ 35 Abs 5 – 8 und 36 ZustG verwiesen.

2.3 Die einzelnen Akteure im Zustellsystem

Grundsätzlich können beliebig viele Personen bzw Organisationen an diesem Zustellsystem als Anbieter oder als Nachfrager teilnehmen und die bereitgestellten Leistungen für sich in Anspruch nehmen. Jeder Teilnehmer (Akteur) hat jedoch eine bestimmte Rolle innerhalb dieses Zustellsystems, aus welcher bestimmte gesetzliche oder vertragliche Rechte und Pflichten resultieren.

2.3.1 Zustelldienst

Ein Zustelldienst im Bereich der elektronischen Zustellung ist gem § 2 Z 7 ZustG „*ein elektronischer Zustelldienst im Anwendungsbereich des 3. Abschnitts des Zustellgesetzes“*. Dabei handelt es sich um eine juristische Person, die vom Bundeskanzler auf Grund eines Antrags eine Zulassung als elektronischer Zustelldienst erhalten hat (vgl Kapitel 1.6) und die infolgedessen Zustellleistungen gem § 29 Abs 1 ZustG erbringen darf. Jeder dieser Zustelldienste darf entsprechend den Bestimmungen des Zustellgesetzes elektronische Dokumente rechtsverbindlich zustellen und die Erbringung solcher Leistungen am Markt anbieten. Über die Erbringung von Zustellleistungen gemäß dem ZustG hinaus ist es einem Zustelldienst erlaubt, auf privatrechtlicher Basis weitere Dienstleistungen entgeltlich anzubieten (§ 29 Abs 3 ZustG).

2.3.2 Ermittlungs- und Zustelldienst

Beim Ermittlungs- und Zustelldienst (EuZD) handelt es sich um einen „gewöhnlichen“ zugelassenen Zustelldienst, der Zustellleistungen gem § 29 Abs 1 ZustG erbringen darf. Darüber hinaus erbringt dieser Zustelldienst auch die Ermittlungs- und Verrechnungsleistung gemäß § 29 Abs 2 ZustG (§ 2 Z 8). Die beiden Leistungen dürfen ausschließlich von diesem einen Akteur im gesamten Zustellsystem erbracht werden.

2.3.3 Behörden im Zuge der Hoheitsverwaltung

Dabei handelt es sich um eine juristische Person, die im Zuge staatlicher Tätigkeit das Zustellsystem für die hoheitliche Zustellung elektronischer Dokumente in Anspruch nimmt. Möchte die Behörde eine Ausfertigung in elektronischer Form mittels eines elektronischen Zustelldienstes rechtsverbindlich zustellen, so hat sie dies in der Zustellverfügung (§ 5 ZustG) entsprechend zu verfügen. Eine Zustellung über einen elektronischen Zustelldienst ist jedoch nur dann möglich, wenn der Empfänger bei einem solchen angemeldet ist[47], die elektronische Zustellung zum aktuellen Zeitpunkt nicht ausgeschlossen hat[48] und die Behörde die zuzustellenden Dokumente in jenem datentechnischen Dateiformat erzeugen kann, welches der Empfänger angegeben hat.[49]

2.3.4 Versender auf privatrechtlicher Basis

Neben Behörden im Zuge der Hoheitsverwaltung können auch Behörden im Zuge der Privatwirtschaftsverwaltung oder sonstige Personen elektronische Dokumente unter Verwendung des Zustellsystems an bestimmte Empfänger übermitteln[50]. In einem solchen Fall handelt es sich jedoch nicht um die Erbringung einer Zustellleistung iSd § 29 Abs 1 ZustG, sondern ausschließlich um eine auf privatrechtlicher Grundlage ausgeführte Dienstleistung. Nichtsdestotrotz darf auch in diesem Fall die Ermittlungsleistung analog zur hoheitlichen Zustellung in Anspruch genommen werden (§ 29 Abs 3 ZustG).

2.3.5 Kunde

Für die Rolle des *Kunden* sieht das ZustG in § 2 Z 9 eine Legaldefinition vor: „*Person, gegenüber der sich ein elektronischer Zustelldienst zur Zustellung behördlicher Dokumente verpflichtet hat.“* Alleine auf Grund des Wortlauts lässt sich anhand dieser Definition noch nicht erkennen, ob sich der Zustelldienst gegenüber einer Behörde zur Durchführung einer Zustellung verpflichten soll und für den potentiellen Empfänger nur ein Postfach bereithalten muss oder sich lediglich gegenüber dem potentiellen Empfänger zur Durchführung von Zustellungen verpflichtet. Interpretiert man diese Legaldefinition alleine auf Grund ihres Wortlauts, lässt diese Norm beide Deu-

[47] § 34 Abs 1 Z 1 ZustG.
[48] §§ 34 Abs 1 Z 2 iVm 33 Abs 2 2. Satz ZustG.
[49] § 34 Abs 1 lS ZustG.
[50] Hier wäre der Begriff der „Zustellung“ nicht zutreffend.

tungen zu. Wirft man jedoch einen Blick in die Erl zur RV 294 so zeigt sich, dass der Gesetzgeber mit der Legaldefinition des Kunden in der neuen Fassung des ZustG eine Klarstellung in der Hinsicht anstrebte, dass nicht weiter die beiden Rechtsbegriffe „Kunde“[51] und „Angemeldeter“[52] wie idF BGBl I 10/2004 Verwendung finden sollen, sondern „Kunde“ als einheitliche Terminologie zur Verwendung kommen soll. Gemäß den Erl seien in beiden Fällen jene Personen gemeint, „die mit dem Zustelldienst vertraglich vereinbart haben, dass er an sie nach den näheren Bestimmungen dieses Bundesgesetzes behördliche Dokumente zustellt“.[53] Auch § 28 Abs 1 Z 2 ZustG idF BGBl I 10/2004 verwendete im Zusammenhang mit der Zustellleistung den Terminus der „vertraglichen Vereinbarung“ zwischen Kunde und Zustelldienst, jedoch wurde dieser mit der Novelle des ZustG (BGBl I 5/2008) nicht beibehalten. In der aktuell gültigen Fassung findet sich die ausdrückliche Klarstellung, dass es sich bei dem Rechtsverhältnis zwischen dem Angemeldeten und dem Zustelldienst um einen zivilrechtlichen Vertrag handelt, somit nicht mehr, jedoch wird man auf Grund historischer Interpretation davon ausgehen müssen, dass die aktuell gültige Legaldefinition des Kunden in § 2 Z 9 ZustG in diesem Sinne verstanden werden muss. Dieses Ergebnis bestätigt auch eine systematische Interpretation, denn die Anmeldung bei einem Zustelldienst gem § 33 Abs 1 ZustG und die Verpflichtung zur unverzüglichen Bekanntgabe von Änderungen von Daten gem Abs 2 können sich nur auf einen potentiellen Empfänger von Dokumenten beziehen, nicht jedoch auf eine Behörde als Absender. Damit scheidet eine Interpretation in der Form aus, dass die zustellenden Behörden „Kunden“ iSd § 2 Z 9 ZustG sein können, was jedoch nahe liegend wäre, da der Zustelldienst als Verwaltungshelfer der Behörde bei der Durchführung des Zustellvorgangs anzusehen ist und was die Notwendigkeit eines Rechtsverhältnisses zwischen diesen beiden Parteien nach sich zieht (vgl Kapitel 3.2). Diese Regelung kann sich somit nicht auf das Rechtsverhältnis zwischen zustellender Behörde und Zustelldienst beziehen sondern nur zwischen potentiellem Empfänger und Zustelldienst, wodurch das ZustG eine Regelung des rechtlichen Verhältnisses zwischen zustellender Behörde und Zustelldienst vermissen lässt.

[51] Vgl § 30 Abs 2 und 3 ZustG aF.
[52] Vgl §§ 32 Abs 1 und 33 Abs 2 ZustG aF.
[53] Erl zur RV 294 BlgNr 23. GP, 17.

2.3.6 Empfänger

Streng zu unterscheiden vom Rechtsbegriff des *Kunden* ist jener des *Empfängers*. Unter einem Empfänger versteht § 2 Z 1 ZustG *„die von der Behörde in der Zustellverfügung (§ 5) namentlich bezeichnete Person, in deren Verfügungsgewalt das zuzustellende Dokument gelangen soll“*. Auf diese strenge Unterscheidung weisen auch die EB nochmals ausdrücklich hin.[54] Von einem Empfänger spricht man folglich immer dann, wenn die Behörde bereits eine Zustellverfügung erlassen hat und ein Dokument einer individualisierten Person hoheitlich zugestellt werden soll. Im Unterschied zu einem Empfänger ist eine Person bereits dann Kunde, wenn sie sich gem § 33 ZustG bei einem Zustelldienst angemeldet hat. Dass (irgend)eine Behörde eine Zustellverfügung für diese Person erlassen hat, ist für diese Qualifikation nicht notwendig. Somit ist eine Person für jene Zeitspanne, innerhalb welcher sie bei einem Zustelldienst angemeldet ist, stets Kunde. Soll ihr innerhalb dieses Zeitraums auch ein behördliches Dokument zugestellt werden, ist sie für den Zeitraum der Erbringung der Zustellleistung durch den Zustelldienst auch Empfänger.

2.3.7 Berechtigter

Analog zu Versendern auf privatrechtlicher Basis kann jede Person neben der Einwilligung in die Durchführung elektronischer Zustellungen auch (gewöhnliche) zivilrechtliche Vereinbarungen mit dem Zustelldienst über die Erbringung sonstiger Dienstleistungen treffen. Auch für diesen Fall würde sich auf Grund eines allgemeinen Begriffsverständnisses die Bezeichnung „Kunde“ anbieten, da im herkömmlichen Wirtschaftssprachgebrauch als Kunden all jene Personen bezeichnet werden, mit welchen ein Unternehmen Geschäftskontakte auf zivilrechtlicher Basis pflegt. In diesem Zusammenhang ist der Begriff jedoch weiter zu verstehen, als dies die Legaldefinition des ZustG vorsieht: Diese betrachtet einen Kunden lediglich als eine Person, der gegenüber eine Zustellleistung gem dem ZustG erbracht werden darf, nicht jedoch solche Personen, denen gegenüber darüber hinausgehende Dienstleistungen auf Grund einer gesonderten zivilrechtlichen Vereinbarung erbracht werden. Daher erscheint in diesem Zusammenhang die Verwendung des Begriffs *Berechtigter* sinnvoll und zutreffend, um Verwechslungen mit der Legaldefinition des ZustG zu vermeiden.

[54] Erl zur RV 294 BlgNr 23. GP, 17.

2.4 Datenschutzrechtliche Aspekte der elektronischen Zustellung

Nachdem nun die Aufgaben der einzelnen Akteure erläutert wurden, sollen auch deren datenschutzrechtliche Rollen festgestellt werden, da sich daraus unterschiedliche gesetzliche Rechte und Pflichten ergeben. Das DSG unterscheidet prinzipiell drei verschiedene Rollen:

Auftraggeber: Auftraggeber ist jene Person, die den Zweck einer Verwendung (Verarbeitung und Übermittlung) personenbezogener Daten festlegt und für die Rechtmäßigkeit der Datenverwendung verantwortlich ist. Der Auftraggeber muss dafür Sorge tragen, dass personenbezogene Daten auf Basis eines gesetzlichen Erlaubnistatbestands gem §§ 7 iVm 8 DSG verarbeitet und übermittelt werden und die Grundsätze einer ordnungsgemäßen Datenverarbeitung gem § 6 DSG eingehalten werden. Werden personenbezogene Daten an andere Auftraggeber übermittelt, so ist die Rechtmäßigkeit der Übermittlung sicherzustellen und zu protokollieren (§§ 7 Abs 2 und 14 Abs 3 DSG). Weiters hat der Auftraggeber seine Datenanwendungen ordnungsgemäß beim Datenverarbeitungsregister (DVR) zu melden (§ 17 ff DSG) und der Geltendmachung von Betroffenenrechten gem § 26 ff DSG zu entsprechen. Es müssen entsprechend angemessene qualitativ hochwertige und dem Stand der Technik entsprechende Datensicherheitsmaßnahmen ergriffen werden, um die Daten vor Verlust, Zerstörung oder unrechtmäßiger Kenntnisnahme (sowohl intern als auch extern) zu schützen (§ 14 DSG).

Dienstleister: Der Dienstleister verarbeitet personenbezogene Daten nur auf Grund einer vertraglichen Vereinbarung mit dem Auftraggeber und ausschließlich zu Zwecken des Auftraggebers. Dafür ist lediglich der Abschluss eines Dienstleistervertrags notwendig, in welchem konkret festgelegt wird, wie die Datenverarbeitung erfolgen muss (§§ 10 und 11 DSG).

Betroffene: Betroffene sind jene (natürlichen oder juristischen) Personen, deren personenbezogene Daten verwendet werden. Ihnen steht das Recht auf Auskunft (§ 26 DSG), Richtigstellung und Löschung (§ 27 DSG) personenbezogener Daten zu.

Für den Bereich der elektronischen Zustellung sieht § 29 Abs 4 1. Satz ZustG vor, dass jeder Zustelldienst bei der Verarbeitung personenbezogener Daten, die für die

Erfüllung der ihm obliegenden Aufgaben notwendig sind, Auftraggeber iSd § 4 Z 4 DSG ist. Somit ist auch der Zustellkopf hinsichtlich der Verarbeitung der Kundendaten der anderen Zustelldienste Auftraggeber[55] und nicht etwa deren Dienstleister oder Dienstleister des BKA (auf Grund des Vertrags resultierend aus dem Ausschreibungsverfahren gem § 32 ZustG). Die Erlaubnis zur Verarbeitung personenbezogener Daten ergibt sich sowohl für (einfache) Zustelldienste als auch für den Zustellkopf somit aus einer gesetzlichen Grundlage (§§ 7 Abs 1 DSG iVm 8 Abs 1 Z 1 DSG iVm 33 Abs 1 und 29 Abs 2 Z 1 ZustG). Auch die Übermittlung von Kundendaten durch einen Zustelldienst an den Zustellkopf (*Aktualisierungsleistung*) oder vom Zustellkopf an eine anfragende Behörde (*Ermittlungsleistung*) basieren auf einer gesetzlichen Grundlage (§§ 7 Abs 2 DSG iVm 8 Abs 1 Z 1 DSG iVm 29 Abs 1 Z 1 oder 34 Abs 1 ZustG).

§ 29 Abs 4 Satz 2 ZustG sieht vor, dass für den Bereich der (behördlichen) elektronischen Zustellung keine Abweichung vom Zweckbindungsgrundsatz (§ 6 Abs 1 Z 2 DSG) zulässig ist. Zweck der Datenverarbeitung ist in diesem Zusammenhang ausschließlich die Durchführung des Zustellvorgangs. Das bedeutet, dass die personenbezogenen Daten von Kunden einzig und allein für den Zweck der Zustellung behördlicher Dokumente verwendet werden dürfen. Das DSG würde zwar unter bestimmten Voraussetzungen die „Weiterverwendung" von personenbezogenen Daten für einen anderen als den ursprünglich intendierten Zweck zulassen, jedoch sind diese Regelungen in diesem Fall auf Grund des ZustG als lex specialis nicht anwendbar. Eine Ausnahme besteht jedoch für den Fall, dass der Kunde vom Zustelldienst neben der elektronischen Zustellung von Dokumenten auch Leistungen auf Grund einer individuellen vertraglichen Vereinbarung in Anspruch nimmt und für diesen (anderen) Zweck solche Daten ebenfalls notwendig sind. In einem solchen Fall kann eine Weiterverwendung vom Berechtigten auch gewünscht sein und für einen solchen Fäll lässt die zitierte Regelung auch eine Ausnahme zu (*„soweit keine besonderen vertraglichen Vereinbarungen mit diesen bestehen"*). Hier ergibt sich der datenschutzrechtliche Erlaubnistatbestand aus der (konkludenten) Einwilligung (§ 8 Abs 1 Z 2 DSG) des Betroffenen oder aus der Notwendigkeit der Speicherung (bzw Weiterverwendung) zur Erfüllung des Vertrags (§ 8 Abs 1 Z 4 iVm Abs 3 Z 4 DSG).

[55] Der Zustellkopf ist ebenfalls ein „herkömmlicher" Zustelldienst, nur mit einem erweiterten Aufgabenbereich (arg „Einer der Zustelldienste hat außerdem…" in § 29 Abs 2 ZustG).

3. Die rechtlichen Beziehungen bei der Zustellleistung

Nachdem im vorherigen Kapitel die im Zustellsystem teilnehmenden Akteure erläutert wurden, gilt es in diesem Zusammenhang nun die Frage zu erörtern, wie sich die rechtlichen Beziehungen zwischen diesen gestalten. Von besonderem Interesse sind die Rechtsbeziehungen zwischen einem Zustelldienst und seinen Kunden sowie zwischen einer zustellenden Behörde und dem Zustelldienst (vgl Abbildung 6 c und d).

Wie bereits in Kapitel 1.5 ausgeführt, handelt der Zustelldienst bei der Durchführung des Zustellvorgangs lediglich als Verwaltungshelfer für die Behörde auf Basis einer Public Private Partnership, wobei der Zustellvorgang einen unselbständigen Teilhoheitsakt darstellt. Im Innenverhältnis zwischen Behörde und Zustelldienst kann sich die Verpflichtung zu einer solchen „Verwaltungshelferschaft" entweder aus einem Bescheid oder einem Vertrag ergeben[56]. Abhängig von der Art der Zustellung kommen für den betrauten Zustelldienst unterschiedliche Regelungen zur Anwendung: Für die physische Zustellung sind dies der 2. Abschnitt des ZustG und das PMG, für die elektronische Zustellung die Regelungen des 3. Abschnitts des ZustG.

3.1 Die Rechtsbeziehung bei der physischen Zustellung

Die physische Zustellung ist gem § 17 Abs 1 PMG im Zuge der Erbringung des Universaldienstes durchzuführen, wodurch jeder Universaldienstbetreiber mit einer solchen betraut werden kann. Dies gilt seit 1. 1. 2011 nun auch für Sendungen bis 50 Gramm, deren Zustellung nun nicht mehr ausschließlich der Österreichischen Post AG im Zuge des reservierten Postdienstes vorbehalten ist. Grundsätzlich sind Postsendungen gem § 6 Abs 3 PMG dann als Universaldienst anzusehen, wenn die zu Grunde liegenden Verträge durch *„Aufgabe in Postbriefkästen oder durch Übergabe der Postsendungen an einem anderen Zugangspunkt abgeschlossen werden"* (zB Postkasten, Postamt, Postpartner, Landzusteller). Behördensendungen sind jedoch immer als Universaldienst zu qualifizieren, unabhängig davon wo sie aufgegeben wurden.[57] Somit ergibt sich für (behördliche) Sendungen aus § 6 Abs 3 PMG, dass die Zustellung auf Grund einer vertraglichen Vereinbarung zwischen Behörde und

[56] *Raschauer*, Allgemeines Verwaltungsrecht, RZ 119.

[57] Vgl Erlass des BMVIT vom 22. 12. 2010 bezüglich der Auslegung der Begriffe „Postdienste", „Universaldienst" und „Dienste im Universaldienstbereich", GZ.: BMVIT-630.036/0002-III/PT1/2010, 3.

Zustelldienst zu erfolgen hat, woraus sich in weiterer Folge gem § 4 ZustG die Stellung des Zustelldienstes als funktionales Organ der Behörde ableitet.

3.1.1 Vertragstyp

Die zu erbringende vertragliche Leistung ist die Zustellung des jeweiligen Dokuments an den in der Zustellverfügung benannten (und idR am Dokument bezeichneten) Empfänger, wodurch es der Behörde folglich auf den konkreten Erfolg ankommt. Der Erfolg zeichnet sich dadurch aus, dass das zuzustellende Dokument vom Zustelldienst entsprechend der Regelungen des ZustG so in den Verfügungsbereich des Empfängers gebracht wird, dass dieser einerseits von dessen Inhalt Kenntnis erlangen kann, andererseits die Zustellwirkungen auch unabhängig davon eintreten, ob der Empfänger vom Inhalt des Dokuments auch tatsächlich Kenntnis nimmt. Aus diesem Grund spricht vieles dafür, dass es sich bei den zwischen Behörde und Zustelldienst zu schließenden Verträgen um Werkverträge iSd §§ 1165 ff ABGB handeln wird.

3.1.2 Vergaberechtliche Aspekte

Da der Vertragsabschluss jeweils durch Übergabe des zuzustellenden Dokuments an den Zustelldienst erfolgt, wird davon auszugehen sein, dass für die Durchführung eines jeden einzelnen Zustellvorgangs ein eigenes (Werk-)Vertragsverhältnis begründet wird. Daraus ergibt sich der Vorteil, dass jede einzelne Zustellung einen separaten Auftragswert darstellt und der Auftrag zur Zustellung eines Dokuments folglich als Direktvergabe iSd §§ 41 f BVergG 2006 erfolgen kann, ohne dass eine Zusammenrechnung von Auftragswerten notwendig wäre.

3.2 Die Rechtsbeziehung bei der elektronischen Zustellung

Anders stellt sich der Sachverhalt gemäß den Materialien zur Zustellgesetznovelle 2004[58] und der hL[59] bei der elektronischen Zustellung dar. Hier ist herrschende Auffassung, dass der Kunde als potentieller Empfänger durch Anmeldung bei einem Zustelldienst ein Vertragsverhältnis mit dem Zustelldienst über die Zustellung behördlicher Dokumente begründe (Abbildung 6, d), die Leistungen gemäß § 29 Abs 1 ZustG

[58] Erl zur RV 252 BlgNR 22. GP, 16 lS.

[59] *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 381; *Feil*, Zustellwesen, 87; *Raschauer/Wessely/Sander*, Österreichisches Zustellrecht, 190; *Larcher*, Zustellrecht, RZ 472; *Hengstschläger*, Verwaltungsverfahrensrecht, RZ 242c.

also vom Zustelldienst auf Grund dieser vertraglichen Vereinbarung mit dem Kunden zu erbringen seien. Ein Vertragsverhältnis zwischen zustellender Behörde und Zustelldienst liege in diesem Fall – im genauen Gegenteil zur physischen Zustellung – nicht vor (Abbildung 6, c).[60] Eine konkrete Begründung dieser Aussage bleiben jedoch sowohl die Materialien („[…] obwohl sie [Anm die zustellenden Behörden] nicht Vertragspartner aller dieser Zustelldienste sind – dies ist vielmehr der Bürger, der sich bei einem – „seinem" – Zustelldienst anmeldet"[61]) als auch die hL schuldig. Es ist anzunehmen, dass davon ausgegangen wird, dass sich Art und Umfang der gesamten vom Zustelldienstes zu erbringenden Leistungen bereits aus dem Vertragsverhältnis zwischen diesem und seinem Kunden ergibt und daher keine Notwendigkeit für weitere zivilrechtliche Verpflichtungen bzw Vereinbarungen im Verhältnis Behörde – Zustelldienst besteht.

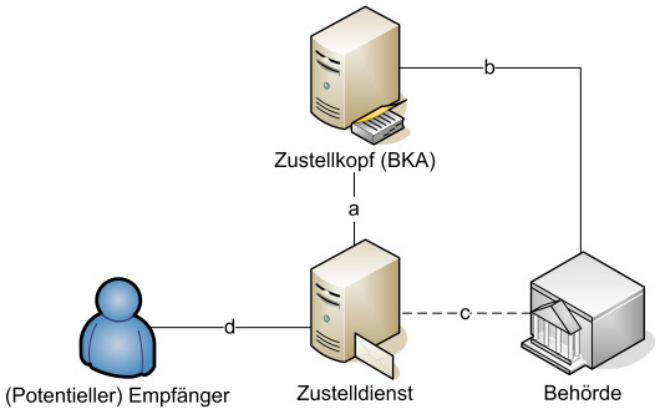

Abbildung 6: Die Akteure im Zustellsystem

3.2.1 Diskussion der herrschenden Ansicht

Die Annahme einer derartigen Ausgestaltung der Rechtsverhältnisse – nämlich dass sich die Verpflichtung des Zustelldienstes zur Durchführung des Zustellvorgangs aus einem zivilrechtlichen Vertrag zwischen potentiellem Empfänger und Zustelldienst und nicht aus einem solchen zwischen zustellender Behörde und Zustelldienst ergebe – wirft mMn sowohl aus praktischen als auch rechtlichen Gesichtspunkten eine Reihe von Problemen und rechtlichen Unzulänglichkeiten auf, welche mit einer konsistenten und praktisch umsetzbaren Anwendung eines solchen elektronischen Zustellsystems nur schwer vereinbar sind. Dies zeigt sich vor allem in Hinblick darauf, dass bezüglich der Inanspruchnahme einer (juristischen) Person des Privatrechts als funktionelles Organ der Behörde kein Unterschied zur physischen Zustellung zu er-

[60] Erl zur RV 252 BlgNR 22. GP, 16 IS; *Feil*, Zustellwesen, 87.
[61] Erl zur RV 252 BlgNR 22. GP, 16 IS.

kennen ist und eine funktionelle Verwaltungshelferschaft – wie bereits ausgeführt – stets einer vertraglichen Grundlage oder eines Bescheides als Basis bedarf. Die rechtlichen Umstände sind – wie *Feil* richtig anmerkt – sowohl beim physischen als auch elektronischen Verfahren „wesensmäßig" die gleichen, *„unabhängig davon, ob sie auf traditionellen Transportwegen oder auf dem neuen Kommunikationsweg Internet vorgenommen"*[62] werden.

Aus diesem Grund wird es unumgänglich sein, dass die Behörde mit dem Zustelldienst zu den üblichen Bedingungen einen Vertrag über die Erbringung der Zustellleistung abschließt. Diesbezüglich trifft den Zustelldienst ein Kontrahierungszwang (vgl Kapitel 3.3.4). Die üblichen Bedingungen hinsichtlich des Entgelts sind für alle Zustelldienste die gleichen, da sich die Höhe des Entgelts aus dem Vergabevertrag gem § 32 Abs 1 ZustG für alle Zustelldienste verbindlich ergibt. Bei einer solchen rechtlichen Konstruktion kommt es mE auch zu keiner Rechtsgestaltung mit Außenwirkung in privatrechtlicher Form, die *Thienel/Schulev-Steindl*[63] für verfassungsrechtlich problematisch erachten. Auch in anderen Bereichen können Unternehmen, welche einem Kontrahierungszwang unterliegen, die Höhe des Entgelts nicht frei festlegen, sondern sind eben an die üblichen Bedingungen gebunden. Im konkreten Fall gibt der Vertrag gem § 32 Abs 1 ZustG die üblichen Bedingungen für alle Zustelldienste verbindlich vor. Die Leistungspflicht des Entgelts ergibt sich für die Behörde direkt aus einer von ihr selbst und freiwillig begründeten vertraglichen Verpflichtung.

a) Verweis auf § 29 Abs 4 ZustG

Zwar sei an dieser Stelle eingeräumt, dass das Zustellgesetz in seiner alten Fassung[64] unmissverständlich auch die Auffassung der hL teilte, da eine der vom Ermittlungs- und Zustelldienst zu erbringenden Leistungen wie folgt definiert wurde: „*Führung eines Verzeichnisses jener Personen, die mit dem Zustelldienst vertraglich vereinbart haben, dass er an sie nach den näheren Bestimmungen dieses Bundesgesetzes behördliche Dokumente zustellt*"[65]. Diese Formulierung wurde jedoch mit der Zustellrechtsnovelle 2007[66] gänzlich beseitigt, was nun neuen Interpretationsspielraum eröffnen könnte. Dennoch halten *Thienel/Schulev-Steindl* an dieser Auffassung

[62] *Feil*, Zustellwesen, 87.
[63] *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 381.
[64] BGBl I 200/1982 idF BGBl I 10/2004.
[65] § 28 Abs 1 Z 1 idF BGBl I 10/2004.
[66] BGBl I 5/2008.

mit Verweis auf § 29 Abs 4 ZustG ohne weitere Begründung fest[67], der wie folgt lautet: „*[…] Sie dürfen die ihnen zur Kenntnis gelangten Daten über ihre Kunden – soweit keine besonderen vertraglichen Vereinbarungen mit diesen bestehen – ausschließlich für den Zweck der Zustellung verwenden. Der Abschluss eines Vertrags über die Zustellleistung sowie der Inhalt eines solchen Vertrags dürfen nicht von der Zustimmung zur Weitergabe von Daten an Dritte abhängig gemacht werden; […]*". Unbestreitbar ist zwar, dass unter die Legaldefinition *Kunde* lediglich potentielle Empfänger behördlicher Dokumente subsumiert werden können (vgl Kapitel 2.3.5), jedoch wird diese Legaldefinition lediglich im ersten zitierten Satz über die strenge Zweckbindung der vom Zustelldienst verwendeten personenbezogenen Daten verwendet. Das bedeutet, dass bereits diese Bestimmung die zweckentfremdete Verarbeitung oder Übermittlung von Daten verbietet, sofern nicht vertraglich mit dem Kunden etwas anderes vereinbart wird. Der zweite zitierte Satz verbietet, dass der Vertragsabschluss über die Zustellleistung an die Bedingung geknüpft wird, dem Zustelldienst die Weitergabe von Daten an Dritte zu erlauben. Dieser Satz bezieht sich aber weder notwendigerweise auf *Kunden* an sich noch auf Kundendaten sondern auf Daten allgemein und auf Daten bezüglich des Inhalts und der Herkunft zuzustellender Dokumente. Diese Formulierung lässt somit offen, ob sie sich auf ein Vertragsverhältnis zwischen Kunde und Zustelldienst oder Zustelldienst und Behörde bezieht. Zwar könnte man mit Verweis auf eine systematische Interpretation argumentieren, dass der zweite Satz in engem Zusammenhang mit dem ersten zu verstehen sei, jedoch befindet sich diese Regelung auch in engem Zusammenhang mit den Regelungen über die Erbringung der Zustellleistung durch den Zustelldienst und verhält sich systematisch gesehen neutral in Hinsicht auf Kunde oder Behörde. Würde sich diese Regelung beispielsweise in § 33 ZustG befinden, wo sie systematisch gesehen ebenso gut aufgehoben wäre, müsste man wohl zu einem anderen Ergebnis kommen. Allein aus dieser Vorschrift kann somit nicht zwangsläufig abgeleitet werden, dass sich der gesetzliche Verweis auf den Abschluss eines Vertragsverhältnisses notwendigerweise auf das Verhältnis Kunde - Zustelldienst bezieht.

b) Interpretation der Legaldefinition des § 2 Z 9 ZustG

Ein zweites Argument, welches für die herrschende Ansicht spricht, ist die Legaldefinition des „*Kunden*" in § 2 Z 9 ZustG*: „Person, gegenüber der sich ein*

[67] *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 381.

elektronischer Zustelldienst zur Zustellung behördlicher Dokumente verpflichtet hat". Diese Regelung besagt mit anderen Worten, dass der Zustelldienst auf Grund seiner (vertraglichen) Vereinbarung mit dem Kunden zur Zustellung behördlicher Dokumente verpflichtet ist. Würde diese Verpflichtung bereits ausschließlich auf Grund des Gesetzes bestehen, wäre einem Zustelldienst eine Selbstverpflichtung durch aktives Tun nicht möglich. Somit wird der herrschenden Ansicht in der Hinsicht wohl gefolgt werden müssen, dass zwischen Kunde und Zustelldienst bei Anmeldung ein Vertragsverhältnis begründet wird, da jede andere Ansicht eine Interpretation contra legem wäre.

Nichtsdestotrotz lassen sich die beiden Ansichten jedoch in der Form vereinen, dass zwar auf Grund des Gesetzes ein Vertragsverhältnis zwischen Zustelldienst und Kunde zu begründen ist, parallel dazu (und somit ergänzend) jedoch ein weiteres Vertragsverhältnis zwischen Behörde und Zustelldienst begründet werden muss, um eine rechtliche Basis für die Verwaltungshelferschaft des Zustelldienstes zu schaffen (vgl Kapitel 1.5). Die Notwendigkeit eines Vertragsverhältnisses zwischen zustellender Behörde und Zustelldienst wird somit aus den dargelegten Gründen wohl trotzdem bejaht werden müssen.

Zu diskutieren bleibt in der Folge, ob die gesetzlich geforderte Begründung eines Vertragsverhältnisses zwischen Kunde und Zustelldienst für eine gesetzeskonforme elektronische Zustellung überhaupt notwendig ist oder ob auf eine solche nicht genauso gut verzichtet werden könnte.

3.2.2 Vergleich mit der physischen Zustellung

In diesem Kapitel soll nun die elektronische Zustellung mit der physischen verglichen werden und auf Gemeinsamkeiten oder Unterschiede hinsichtlich der Rechtsbeziehung zwischen Empfänger/Kunde und Zustelldienst untersucht werden. Als Zustelldienst gem § 2 Z 7 ZustG kommen bestimmte juristische Personen in Betracht, welchen sowohl bei der physischen als auch elektronischen Zustellung dieselbe Rechtsposition eingeräumt wird, da Ziffer 7 bezüglich der Rechtsstellung nicht differenziert. Bei einem Zustelldienst handelt es sich somit in jedem Fall um eine juristische Person, welche im Auftrag von Behörden Zustellungen in funktionaler Hoheitsverwaltung (§ 4 ZustG) für die jeweiligen Behörden durchführt. Die effektive Durchführung eines Zustellvorgangs hat in beiden Fällen entsprechend dem Zustellgesetz zu erfolgen. Abhängig davon, ob es sich um eine physische oder

elektronische Zustellung handelt, kommen jeweils die Regelungen entweder des 2. oder des 3. Abschnitts zur Anwendung. Auch die Regelungen hinsichtlich der Amtsverschwiegenheit[68] und des Schadenersatzes[69] für Schäden, welche bei der Durchführung des Zustellvorgangs durch die jeweiligen Organe verursacht werden, sind weitgehend gleich gelagert.

Die Rechtsbeziehung zwischen Behörde und Zustelldienst beruht bei der physischen Zustellung stets auf einer zivilrechtlichen Vereinbarung, welche den jeweils beauftragten Zustelldienst zur Durchführung des Zustellvorgangs verpflichtet[70]. Dieser hat die Zustellung gemäß der §§ 13 – 27 ZustG durchzuführen (§ 17 Abs 1 PMG) und tritt dem Empfänger gegenüber mit Hoheitsgewalt auf (§ 4 ZustG). Kann ein Dokument nicht zugestellt werden, weil zB der Empfänger die Annahme ohne gesetzlichen Grund verweigert[71] oder seine Anwesenheit verleugnet[72], so kann das zuzustellende Dokument beim Zustelldienst gem § 17 ZustG hinterlegt werden, wodurch die Rechtskraft auch ohne Zutun bzw gegen den Willen des Empfängers eintreten kann.[73] Zusammengefasst kann gesagt werden, dass die Behörde mittelbar unter Zuhilfenahme eines Zustelldienstes hoheitlich an den Empfänger herantritt und die Zustellung nötigenfalls auch ohne dessen Mitwirkung ausschließlich auf Grund des Zustellgesetzes durchgeführt werden kann. Dass für die Setzung eines solchen Hoheitsaktes zuvor eine Einwilligung des Betroffenen oder der Abschluss einer zivilrechtlichen Vereinbarung zwischen Betroffenem und Behörde bzw Betroffenem und Zustelldienst als Organ der Behörde notwendig wäre, ist nicht nachvollziehbar. Die Notwendigkeit einer solchen zivilrechtlichen Vereinbarung würde auch dem Charakter hoheitlichen Handelns zuwider laufen.

Nun stellt sich konsequenter Weise die Frage, warum eine solche zivilrechtliche Vereinbarung im Zuge der elektronischen Zustellung zwischen dem Kunden und dem Zustelldienst, der in der Folge bei der Durchführung des Zustellvorgangs wie ein physischer Zustelldienst hoheitlich als Organ der Behörde handelt, notwendig sein sollte. Es erscheint doch geradezu absurd, dass der Rechtsunterworfene zuvor (freiwillig) eine zivilrechtliche Vereinbarung schließen muss, bevor eine Behörde (auf

[68] Vgl §§ 5 PMG und 29 Abs 5 ZustG iVm 46 Abs 1 bis 4 BDG.
[69] Vgl §§ 17 PMG.
[70] Vgl §§ 6 Abs 2 und 3 iVm 19 PMG.
[71] § 20 Abs 1 ZustG.
[72] § 20 Abs 3 ZustG.
[73] § 17 Abs 3 S 2 ZustG.

Basis dieser Vereinbarung) einen Hoheitsakt gegen den Betroffenen setzen kann bzw darf.

Auch dem Argument der Freiwilligkeit bezüglich der Inanspruchnahme der elektronischen Zustellung, welche somit einen Ausfluss der Vertragsfreiheit darstelle, kann nicht konsequent gefolgt werden, da auch ein physisches Dokument vom Empfänger bedingungslos (und somit „freiwillig“) entgegengenommen werden kann, widrigenfalls ihm dieses durch Hinterlegung zwangsweise zugestellt werden kann. Auch bei der elektronischen Zustellung kann sich der Kunde nach erfolgter Anmeldung nicht „aussuchen“, welche Zustellstücke er entgegennehmen möchte und welche nicht, denn durch Login beim Zustelldienst tritt die Zustellwirkung entsprechend der gesetzlichen Regelungen für alle bereitliegenden Dokumente auch ohne bzw gegen den Willen des Kunden ein.

Zusammengefasst lässt sich kein vernünftiger Grund erkennen, welcher die Notwendigkeit einer abweichenden rechtlichen Beurteilung oder Konstruktion der physischen und elektronischen Zustellung notwendig erscheinen lässt. Der rechtliche Rahmen ist bei beiden Varianten gleich gelagert, nur die Verfahren an sich weichen aus praktischen Gründen voneinander ab. Vergleichbar ist diese Situation mit dem Fall, dass sich jemand ein physisches Postfach mietet, in welches Zustellungen erfolgen sollen: Auch hier wird das Vertragsverhältnis bezüglich einer Zustellung parallel zum Mietvertrag zwischen Behörde und Zustelldienst begründet.

3.2.3 Das Fehlen einer Hauptleistungspflicht

Geht man bei der Anmeldung beim Zustelldienst von der Begründung eines rechtsgeschäftlichen Schuldverhältnisses aus, so stellt sich die Frage, welche Hauptleistungspflichten ein solches Schuldverhältnis charakterisieren. Den Kunden trifft allein dem Wortlaut des ZustG zufolge keinerlei erkennbare Verpflichtung: Dieser kann sich beliebig beim Zustelldienst an- oder abmelden. Abgesehen vom Erfordernis der Verwendung der Bürgerkarte oder der Schriftlichkeit bestehen keinerlei materiellrechtliche Voraussetzungen für eine solche An- oder Abmeldung, es trifft den Kunden keinerlei Entgeltpflicht und auch eine gewisse Bindung des Kunden – beispielsweise in Form von „Kündigungsfristen“ – bestehen nicht. Den Kunden trifft durch die Anmeldung somit keinerlei rechtsgeschäftliche Verpflichtung in Form eines Tuns oder Unterlassens; eine vertragliche Hauptleistungspflicht für den Kunden ist somit nicht erkennbar.

Koziol/Welser führen zur Definition einer Hauptleistungspflicht folgendes aus: *„Zum Schuldverhältnis im weiteren Sinn gehört vor allem die Hauptleistungspflicht. Sie charakterisiert den Vertragstyp, macht das Wesen des Rechtsgeschäftes aus, das von den Parteien gerade ihretwegen geschlossen wird. Im einfacheren Fall trifft die Hauptleistungspflicht nur eine Seite. Es entsteht eine einseitige Verbindlichkeit, bei der ein Teil (der Schuldner) nur verpflichtet, der andere Teil (der Gläubiger) nur berechtigt wird […].“*[74] Dazu *Bydlinski*: *„Wegen der Hauptleistungspflichten (aus der Sicht der Gläubiger: ‚Hauptansprüche') wird der Vertrag geschlossen: […]“.*[75] Verpflichtet zu einer Leistung wäre dem Wortlaut des Zustellgesetzes zu Folge lediglich der Zustelldienst, der sich dem Kunden gegenüber zur Zustellung behördlicher Dokumente verpflichtet hat.[76] Somit könnte es sich gegebenenfalls lediglich um ein zweiseitiges jedoch nur einseitig den Zustelldienst verpflichtendes Schuldverhältnis handeln.

Doch auch für den Zustelldienst stellt sich die Frage, welche konkrete Hauptleistungspflicht diesen aus einem solchen Vertragsverhältnis mit einem Kunden treffen sollte. Die Erbringung einer Zustellleistung kann er gegenüber dem Kunden jedenfalls nicht versprechen, da eine solche in jedem Fall ausschließlich von einer Behörde verfügt (§ 5 ZustG) und durch Begründung eines zivilrechtlichen Vertrags beauftragt werden muss. Der Zustelldienst alleine kann eine solche Hauptleistungspflicht gar nicht erfüllen, denn es liegt ausschließlich im Ermessen einer Behörde, ob sie – auch wenn die technischen Voraussetzungen vorliegen – eine elektronische Zustellung verfügt oder aus Ermessensgründen die physische Zustellung wählt. Die Erfüllung der Hauptleistungspflicht in einem solchen vom ZustG skizzierten Vertragsverhältnis wäre rechtlich unmöglich, da es nicht in der Rechtsmacht eines Zustelldienstes liegt, eine solche Leistung (ohne Zutun der Behörde) zu erbringen. Dem Zustelldienst ist es rechtlich objektiv geradezu unmöglich, sich ohne Zutun einer Behörde die (notwendige) funktionelle Organschaft gem § 4 ZustG zu verschaffen, was dem Zustelldienst aber bereits bei Vertragsabschluss erkennbar ist. Ein solches zivilrechtliches Vertragsverhältnis müsste in Konsequenz gem § 878 Satz 1 ABGB wegen ursprünglicher rechtlicher Unmöglichkeit als absolut nichtig angesehen werden.

---

[74] *Koziol/Welser*, Bürgerliches Recht II, 3.
[75] *Bydlinski*, Bürgerliches Recht I, RZ 5/5.
[76] § 2 Z 9 ZustG.

Dies führt im Endeffekt zu der absurden Situation, dass das Zustellgesetz eine rechtliche Konstruktion vorzeichnet, welche von Gesetzes wegen gar nicht existieren kann.

Abgesehen davon könnte die Hauptleistungspflicht des Zustelldienstes somit lediglich darin bestehen, dass er für den Kunden eine „virtuelle Zustellsphäre“ (kostenlos) bereitstellt, in welcher ein Zustellvorgang ausgeführt werden könnte.[77] Doch auch in einem solchen Fall muss der Zustellvorgang von der Behörde durch Begründung eines (zusätzlichen) zivilrechtlichen Vertrags über die Erbringung der Zustellleistung mit dem Zustelldienst abgeschlossen werden, um eine Basis für die Verwaltungshelferschaft des Zustelldienstes zu schaffen.

3.2.4 Wahlfreiheit der Kommunikationsart im E-Government

Geht man nun wie dargelegt davon aus, dass zwischen Kunde und Zustelldienst nicht notwendigerweise ein zivilrechtlicher Vertrag abgeschlossen werden muss, stellt sich in weiterer Folge die Frage, wie eine Anmeldung eines Kunden bei einem Zustelldienst gem § 33 ZustG rechtlich zu qualifizieren ist.

Die einzig für diesen Fall wirklich tauglich erscheinende Regelung findet sich im E-Government-Gesetz, welches dem Bereich des öffentlichen Rechts zuzuordnen ist und Regelungen für elektronisches Behördenhandeln sowie elektronische Kommunikationen mit Behörden trifft (vgl § 1 E-GovG). § 1 Abs 1 E-GovG normiert das **Prinzip der Wahlfreiheit des Kommunikationskanals**: „*Dieses Bundesgesetz dient der Förderung rechtserheblicher elektronischer Kommunikation. Der elektronische Verkehr mit öffentlichen Stellen soll unter Berücksichtigung grundsätzlicher Wahlfreiheit zwischen Kommunikationsarten für Anbringen an diese Stellen erleichtert werden.“*

§ 1 Abs 1 E-GovG sieht somit vor, dass Rechtsunterworfene grundsätzlich die Wahl haben sollen, neben den herkömmlichen Kommunikationskanälen auch elektronische Dienste für die Kommunikation mit öffentlichen Stellen zu nutzen. Diese Regelung stellt somit eine *Opt-In-Möglichkeit* dar, der Einschreiter ist jedoch nicht verpflichtet, sich eines solchen elektronischen Kommunikationskanals zu bedienen. Somit kann ein Einschreiter freiwillig – unter Beachtung der gesetzlichen Rahmenbedingungen – elektronisch an die Behörde herantreten, umgekehrt kann er

[77] Vgl Erl zur RV 252 BlgNR 22. GP, 17 zu § 34.

aber auch der Behörde gegenüber seine Einwilligung erteilen, dass auch diese elektronisch an ihn herantreten darf. Zwar spricht diese Regelung von der „Wahlfreiheit der Kommunikationsarten für Anbringen“, worunter bei strenger Interpretation des Wortlauts nur die Kommunikation „zur“ Behörde zu subsumieren wäre, jedoch ist davon auszugehen, dass diese Bestimmung extensiv für alle Kommunikationsformen zur als auch von der Behörde anzuwenden ist.[78] Diese Ansicht lässt sich sowohl mit einer systematischen als auch teleologischen Interpretation untermauern: Einerseits regelt das E-GovG in den §§ 19 f auch die Amtssignatur, welche auf elektronische Ausfertigungen aufzubringen ist, die dem Empfänger nahe liegender Weise auch elektronisch übermittelt werden können sollen. Andererseits bezieht sich § 1 E-GovG auf das gesamte E-GovG, was aus seiner Überschrift *„Gegenstand und Ziele des Gesetzes“* erkennbar ist. Auch die EB deuten sowohl in ihrem Wortlaut auf dieses Ergebnis, als auch dadurch, dass sie in den Erl zu § 1 auf die Abschnitte 2 sowie 4 bis 6 verweisen, in welchen auch die Amtssignatur geregelt ist: „*Im Mittelpunkt der Regelungen eines E-Government-Gesetzes stehen naturgemäß Fragen der elektronischen Kommunikation mit und zwischen öffentlichen Stellen (2. Abschnitt und 4. bis 6. Abschnitt).“*[79] Weiters wird im Allgemeinen Teil explizit auf die elektronische Zustellung verwiesen.[80] Des Weiteren kommt auch das Konzept der Bürgerkarte (§§ 4 ff E-GovG) bei der elektronischen Zustellung sowohl bei der Anmeldung beim Zustelldienst (§ 33 ZustG) als auch bei der Abholung bereitgehaltener Dokumente (§ 35 Abs 3 ZustG) zum Einsatz, was in der Form zu deuten ist, dass das E-GovG auch für eine elektronische Kommunikation von der Behörde zum Bürger anwendbar ist. Zur Klarstellung sollte somit die Wortfolge „für Anbringen an diese Stellen“ de lege ferenda aus § 1 Abs 1 E-GovG entfernt werden.

Für die Zustimmung zu einem bestimmten Verhalten eines Dritten durch den Betroffenen ist im Allgemeinen nicht notwendigerweise die Begründung eines zivilrechtlichen Vertragsverhältnisses erforderlich. Dies zeigt sich beispielsweise sehr deutlich bei der Zustimmung zur Verwendung personenbezogener Daten durch den Betroffenen (§§ 8 Abs 1 Z 2 oder 9 Z 6 iVm 4 Z 14 DSG). Bei einer solchen Zustimmung handelt es sich um eine Willenserklärung, da sie auf die Herbeiführung

[78] *Dohr/Pollirer/Weiss*, E-Government-Gesetz, 3; Vgl Erl zur RV 294 BlgNR 23. GP, 2 2. Punkt.
[79] Erl 252 BlgNR 22. GP, 5.
[80] Erl 252 BlgNR 22. GP, 4.

von Rechtsfolgen abzielt, nämlich dass die Behörde rechtsgültig elektronische Zustellungen vornehmen kann. Da sowohl das ZustG als auch das E-GovG dem öffentlichen Recht zuzuordnen ist, kann es sich bei einer solchen Willenserklärung lediglich um eine öffentlich-rechtliche Erklärung handeln. Der die Zustimmung zur elektronischen Zustellung bildende positive Willensakt ist somit die Anmeldung beim Zustelldienst gem § 33 ZustG, was in der Folge darauf hindeutet, dass es sich dabei nicht um die Begründung eines zivilrechtlichen Vertrags handeln kann. Auch im Zweifel ist davon auszugehen, dass eine Willenserklärung eine öffentlich-rechtliche und keine zivilrechtliche ist (VwSlg 6272 A/1964). Sieht man in der Anmeldung beim Zustelldienst lediglich eine auf § 1 Abs 1 E-GovG basierende rechtsgestaltende öffentlich-rechtliche Willenserklärung in der Form einer Einwilligung in die elektronische Zustellung anstatt einer Willenserklärung zur Begründung eines zivilrechtlichen Vertragsverhältnisses, so erklärt dies auch das Fehlen einer vertraglichen Hauptleistungspflicht (vgl Kapitel 3.2.3).[81]

Zu betonen ist an dieser Stelle jedoch, dass sich eine solche Willenserklärung nicht an den Zustelldienst sondern nur an die zustellende Behörde richten kann, da ausschließlich sie auf Grund dieser Einwilligung in die Rechtsmacht versetzt wird, sich der elektronischen Zustellung zu bedienen und eine solche zu verfügen. Damit eine solche Willenserklärung nicht jeder einzelnen Behörde gegenüber abgegeben werden muss, wurde der Zustellkopf als zentraler Verzeichnisdienst geschaffen, welcher all jene Personen verwaltet, die ihre Einwilligung in die elektronische Zustellung abgegeben haben, und dies gegenüber Behörden beauskunftet. Der Zustellkopf dient somit als Bote zur Übermittlung dieser Willenserklärung an die jeweils anfragende Behörde.

Zur Verifizierung sollen diese Annahmen und Aussagen anhand der wesentlichen Regeln in *Raschauer* RZ 1252 ff gegengeprüft werden:

- Bei der Anmeldung beim elektronischen Zustelldienst handelt es sich um eine ausdrückliche Willenserklärung, welche die Einwilligung in die elektronische Zustellung von Dokumenten darstellt. Ein anderer Erklärungswert kann einer solchen Anmeldung praktisch nicht unterstellt werden (RZ 1253).
- Die Rechts- und Handlungsfähigkeit richtet sich gem § 9 AVG nach bürgerlichem Recht, wodurch organschaftliche Vertreter eine Willenserklärung

[81] Vgl *Raschauer*, Allgemeines Verwaltungsrecht, RZ 1234 ff.

für die juristische Person abgeben können. Somit kann durch Anmeldung eines organschaftlichen Vertreters beim Zustelldienst die Willenserklärung der juristischen Person zugerechnet werden (RS 1254).

- Eine Willenserklärung kann auch durch einen Boten übermittelt werden. Einen solchen bildet bei der elektronischen Zustellung der Zustellkopf, welcher die Willenserklärung (Einwilligung) der bei einem elektronischen Zustelldienst angemeldeten Empfänger im Zuge der Adressierbarkeitsabfrage an die Behörde weiterleitet (RZ 1254, VwGH 96/03/0008 vom 26. 11. 1997).
- Da die Adressierbarkeitsabfrage vor Verfügung der Zustellung oder ggf im Zuge einer Eventualanordnung erfolgen muss, geht diese Willenserklärung der Behörde stets auch rechtzeitig zu (RZ 1255).

3.2.5 Ergebnis

Der Vertragsabschluss bezüglich der Durchführung des Zustellvorgangs zwischen Behörde und Zustelldienst ist rechtlich erforderlich und erfolgt analog zum PMG durch Übergabe der zuzustellenden Dokumente an einen bestimmten Zugangspunkt (vgl § 6 Abs 3 PMG). Diesen Zugangspunkt bildet bei der elektronischen Zustellung die technische Schnittstelle des jeweiligen Zustelldienstes zur Übernahme von elektronischen Dokumenten. Sobald die Übernahme durch das Empfangssystem bestätigt wurde, kann der Vertrag über die Zustellleistung als abgeschlossen angesehen werden. Die Vertragsannahme ergeht in diesem Fall als „automatisierte Willenserklärung“ in Form einer Status- bzw Erfolgsmeldung an das absendende Computersystem, welche dem Betreiber des Computersystems zuzurechnen ist[82] (vgl Kapitel 3.3.2). Ein Vertragsabschluss zwischen potentiellem Empfänger und Zustelldienst ist nicht notwendig, da eine öffentlich-rechtliche Willenserklärung für die Einwilligung in die elektronische Zustellung als ausreichend angesehen werden kann und darüber hinaus im Verhältnis zwischen diesen Parteien keine vertraglichen Hauptleistungspflichten existieren.

[82] Vgl *Zankl*, Rechtsqualität und Zugang von Erklärungen im Internet, ecolex 2001, 344; *Ortner*, Internet und Recht in *Barta*, onlineLehrbuch Zivilrecht http://www.uibk.ac.at/zivilrecht/buch/kap2_0.xml?sectionview=true;section=4, 12. 6. 2011.

3.3 Rechtliche Qualifikation des Zustellvertrags

Geht man nun wie dargelegt davon aus, dass jedenfalls ein Vertrag zwischen Behörde und Zustelldienst über die Erbringung der Zustellleistung notwendig sein wird (unabhängig von der Frage, ob zwischen Zustelldienst und Kunde nun zusätzlich ein zivilrechtlicher Vertrag zu schließen ist oder nicht), stellt sich analog zur physischen Zustellung (vgl Kapitel 3.1.1) die Frage, welcher Vertragstyp für ein solches Rechtsverhältnis in Frage kommen könnte und wie dieses Vertragsverhältnis abgeschlossen wird.

3.3.1 Der Vertragstyp für die Erbringung der Zustellleistung

Entsprechende einschlägige Literatur oder Judikatur existiert bezüglich der Beantwortung dieser Frage aktuell noch nicht, das einzige höchstgerichtliche Urteil, welches einen rechtsqualitativ relativ ähnlichen Sachverhalt behandelt, ist das Urteil des OGH (6 Ob 69/05y) vom 21. 4. 2005 bezüglich der Frage, welchem Vertragstyp die Rechtsverhältnisse zwischen einem Mobilfunkanbieter und seinen Kunden unterliegen. Im Vergleich zur Nutzung eines Mobilfunknetzes handelt es sich auch bei der elektronischen Zustellung um eine (relativ) autonom agierende voll automatisierte technische Kommunikationsinfrastruktur, welche unterschiedliche Personen zur Übermittlung von Willensmitteilungen oder sonstigen Daten nutzen. Die rechtsqualitative Ähnlichkeit ergibt sich daraus, dass sowohl bei der Nutzung eines Mobilfunknetzes durch einen Kunden als auch bei der Nutzung eines elektronischen Zustelldienstes durch eine Behörde jeweils eine technische Infrastruktur in einer bestimmten leistungsspezifischen Ausprägung vom jeweiligen Betreiber zur Verfügung gestellt wird, welche der Nutzer in der bestehenden Form in Anspruch nehmen und benutzen kann. In beiden Fällen ist es einem Nutzer jedoch nicht möglich, die Leistungen und technischen Funktionalitäten der Infrastruktur individuell (zB durch entsprechende Vertragsgestaltung) zu beeinflussen, sondern er kann diese lediglich in der vom Betreiber angebotenen Form für seine Zwecke nutzen.

Der OGH kam mit Verweis auf *Zankl*[83] zum Ergebnis, dass es sich dabei um einen Mischvertrag handle, welcher werkvertragliche, dienstvertragliche als auch mietrechtliche Elemente aufweise, wobei das werkvertragliche Element deutlich hinter das mietvertragliche zurücktrete. Dies wurde damit begründet, dass dem

[83] *Zankl*, Qualifikation und Dauer von Mobilfunkverträgen, ecolex 2005, 29.

Nutzer lediglich ein voll automatisiertes Kommunikationsnetz samt seinen technischen Einrichtungen in seiner bestehenden Form zur Nutzung (Austausch von Sprache und Daten) zur Verfügung gestellt und daher kein Werk hergestellt werde.[84] Insbesondere schulde der Netzbetreiber keinen konkreten Erfolg, wobei Gewährleistungsansprüche dem Urteil zu Folge allenfalls gegen die Annahme eines Dienstvertrags ins Treffen geführt werden können. Auch wenn man von der Herstellung eines konkreten Erfolges ausgehe, trete das werkvertragliche Element deutlich hinter das mietvertragliche zurück. Weiters führte der Gerichtshof aus, dass die Beurteilung stets im Einzelfall erfolgen müsse, da immer auf die konkrete Individualvereinbarung abzustellen sei: *„Ähnlich wie beispielsweise ein Anstellungsvertrag von Vorstandsmitgliedern als Dienstvertrag, als freier Dienstvertrag oder auch als Werkvertrag vertraglich gestaltet werden kann, kommt es auch hier bei der Beurteilung des Mobilfunkvertrags entscheidend auf die vertraglichen Umstände des Einzelfalls an, also darauf, welcher Vertragstyp den Kern des Vertragsverhältnisses nach dem Parteiwillen ausmacht.“* Eine allgemein gültige Aussage, welchen Vertragstyp die Vereinbarung über die Erbringung der Zustellleistung darstellt, kann analog folglich nicht getroffen werden.

Nichtsdestotrotz wird in Übereinstimmung mit der Argumentation im Urteil davon auszugehen sein, dass es sich bei der elektronischen Zustellung ebenfalls um einen Mischvertrag handeln wird, wobei mE jedoch davon auszugehen ist, dass in diesem Fall das werkvertragliche Element überwiegen muss. Dies begründet sich damit, dass es der Behörde geradezu auf den konkreten Erfolg ankommen wird, nämlich der gesetzeskonformen Durchführung des Zustellvorgangs und folglich auf den Eintritt der Zustellwirkung. Gegen das Vorliegen eines Mietvertrags spricht, dass der Zustelldienst ja als Organ der Behörde tätig wird und dieser Vertrag die Basis für die funktionelle Organstellung des Zustelldienstes darstellt. Da der Zustelldienst als Organ der Behörde und somit in ihrem Auftrag handelt, impliziert dies auch ein gewisses aktives Tun, wodurch mit der bloßen Gebrauchsüberlassung einer Gesamtsache iSd § 1090 ABGB an die Behörde nicht das Auslangen gefunden werden kann. Würde man die gegenteilige Auffassung vertreten, würde sich die Behörde bei einer elektronischen Zustellung lediglich einer Sache bedienen und daher selbst den Zustellvorgang durchführen. In einem solchen Fall würde die

[84] Vgl *Zankl*, Qualifikation und Dauer von Mobilfunkverträgen, ecolex 2005, 29.

Regelung des § 4 ZustG, welche auch für elektronische Zustelldienste anwendbar ist, ad absurdum geführt werden.

Geht man vom Vertragstyp eines Werkvertrags bzw eines Mischvertrags mit überwiegenden werkvertraglichen Elementen aus, wird jeder Zustellvorgang im Rahmen eines autonomen Vertragsverhältnisses durchgeführt und könnte daher analog zur physischen Zustellung mittels Direktvergabe iSd BVergG 2006 erfolgen. Anderenfalls würden alle elektronischen Zustellvorgänge innerhalb ein und desselben Vertragsverhältnisses (Mietvertrag) erfolgen, wodurch die Notwendigkeit einer Ausschreibung eintreten könnte.

Eine ähnliche Regelung im ZustG, welche dies wie § 6 Abs 3 PMG in Bezug auf die physische Zustellung analog für die elektronische Zustellung klarstellt, wäre daher wünschenswert.

3.3.2 Der Vertragsabschluss

Wie bei jedem Vertragsabschluss kommt auch das Vertragsverhältnis zwischen Behörde und Zustelldienst über die Erbringung der Zustellleistung durch Angebot und Annahme (ggf unter Einbeziehung der AGB, welche im Zuge der Zulassung gem § 30 Abs 1 ZustG genehmigt wurden) zustande. Im Fall der elektronischen Zustellung stellt somit die Übermittlung der zuzustellenden Dokumente an den Zustelldienst über die entsprechende normativ spezifizierte Schnittstelle (vgl ZUSEMSG, Kapitel 8) gleichzeitig auch das Angebot dar. Gemäß der Schnittstellenspezifikation muss das Zustellsystem des Zustelldienstes an die absendende Behörde eine entsprechende Rückmeldung geben, ob das Dokument erfolgreich übernommen werden konnte oder ob ein Fehler auftrat. Diese Rückantwort stellt gleichzeitig auch die Annahme bzw Ablehnung dieses Angebots dar. Dass der Vertragsabschluss ausschließlich voll automatisiert von Computersystemen durchgeführt wird, stellt rechtlich kein Problem dar. Die der jeweiligen technischen Operation innewohnende rechtliche Willenserklärung ist jener Person zuzurechnen, welche sich der Funktionalität des Systems bedient. Dies hat *Zankl*[85] bereits ausführlich begründet dargelegt und dieser Ansicht ist mMn auch uneingeschränkt zu folgen. Auf Seiten des Zustelldienstes ist dieses technische System die Zustellapplikation, auf Seiten der Behörde die absendende Applikation

[85] *Zankl*, Rechtsqualität und Zugang von Erklärungen im Internet, ecolex 2001, 344.

(zB MOA-ZS). Darüber hinaus darf nicht übersehen werden, dass auch jeder elektronische Zustellvorgang idR von einer natürlichen Person ausgelöst wird (zB durch Klick in einem ELAK-System).

3.3.3 Inhalt des Vertragsverhältnisses

§ 29 Abs 1 ZustG listet eine Reihe von Teilleistungen auf, welche in Summe die „Zustellleistung" darstellen. Diese Regelung birgt jedoch praktisch die Schwierigkeit in sich, dass sich die einzelnen Teilleistungen in drei Gruppen unterteilen lassen, wobei sich für jede Gruppe unterschiedliche rechtliche Implikationen bzw Konsequenzen ergeben, die sich nur schwer vereinbaren lassen:

- Allgemeine Leistungen (Ziffern 1, 2, 3, 6)
- Zustellleistungen (Ziffern 4, 5, 7, 8, 9)
- Leistungen auf Anforderung des Empfängers (Ziffern 10, 11)

A*llgemeine Leistungen* müssen von jedem Zustelldienst erbracht werden und zwar unabhängig davon, ob jemals nur eine einzige Behörde eine elektronische Zustellung verfügt. Die Erbringung dieser Leistungen ist notwendige Voraussetzung für die Erteilung und Aufrechterhaltung einer Zulassung gem § 30 ZustG und daher unabhängig von einer vertraglichen Vereinbarung bereits von Gesetzes wegen zu erfüllen. Die Voraussetzungen für die Erbringung einer Zustellleistung sind somit unabhängig von der tatsächlichen Durchführung einer Zustellung zu schaffen und aufrecht zu erhalten. Erfüllt ein Zustelldienst folglich die ihm obliegenden gesetzlichen (allgemeinen) Leistungspflichten nicht oder nicht ordnungsgemäß, so ist – unabhängig davon ob jemals eine Zustellung verfügt wurde – die Zulassung vom Bundeskanzler zu widerrufen (§ 30 Abs 4 ZustG).[86] Somit kann der Zustelldienst für die Erbringung dieser Allgemeinen Leistungen – im Widerspruch zu § 29 Abs 1 aE ZustG – unmittelbar kein Entgelt von einer Behörde verlangen, sondern die dadurch entstehenden Kosten nur indirekt über die Durchführung von Zustellvorgängen amortisieren. Verfügt keine Behörde je eine einzige Zustellung, erhält der Zustelldienst für die Erbringung dieser Leistungen auch nie ein Entgelt. Diese Allgemeinen Leistungen können somit nicht Inhalt eines Vertrags zwischen Behörde und Zustelldienst sein, da diese bereits auf Grund des ZustG zu erbringen sind.

[86] Vgl Erl zur RV 294 BlgNr 23. GP, 22.

Die *Zustellspezifischen Leistungen* hingegen sind nur dann zu erbringen, wenn eine Behörde auch tatsächlich die Ausführung eines Zustellvorgangs beauftragt. Sie bilden somit die hoheitlich durchzuführenden Einzelschritte, um das zuzustellende Dokument in den Machtbereich des Empfängers zu übermitteln, und sind damit als Teilschritte des gesamten Hoheitsakts der zustellenden Behörde zuzurechnen. Diese Leistungen stellen somit auch die Hauptleistungspflichten aus dem Vertrag zwischen Behörde und Zustelldienst dar, da sie – im Gegensatz zu den Allgemeinen Leistungen – nicht bereits von Gesetzes wegen erbracht werden müssen, sondern nur auf Grund der vertraglichen Vereinbarung. Für die Erbringung dieser Leistungen gebührt dem Zustelldienst auch unmittelbar das zu entrichtende Entgelt.
Die dritte Gruppe bilden die *Leistungen auf Anforderung des Empfängers*, da sie nicht unmittelbar mit dem Zustellvorgang in Verbindung stehen. Die Verpflichtung zu deren Erbringung ergibt sich aus einer eigenständig abzuschließenden zivilrechtlichen Vereinbarung zwischen Kunde und Zustelldienst, da hierfür auch der Kunde das Entgelt zu leisten hat (§ 29 Abs 1 lS ZustG, vgl Kapitel 11.3). Die Erbringung dieser Leistungen wird analog zu jenen der *Zustellspezifischen Leistungen* einem Kontrahierungszwang unterliegen (vgl Kapitel 3.3.4).

Zusammengefasst lässt sich feststellen, dass sich die jeweiligen Gruppen entweder bezüglich ihres rechtlichen Verpflichtungsgrundes oder der jeweiligen Parteien unterscheiden. Alle diese Leistungen gleichermaßen als Teilleistungen einer einzigen Zustellleistung zu sehen (wie dies § 29 Abs 1 ZustG tut), lässt sich somit rechtlich nur schwer konsequent aufrecht halten. Nahe liegender wäre es, die Legaldefinition der „Zustellleistung“ auf die *Zustellspezifischen Leistungen* zu reduzieren und die *Allgemeinen Leistungen* als gesetzlich zu erbringende Leistungen sowie *Leistungen auf Anforderung des Empfängers* je in einen eigenen Absatz „auszugliedern“.

Diese Unterscheidung ist neben der Frage zu den konkreten Hauptleistungspflichten im Vertrag zwischen Behörde und Zustelldienst weiters auch wesentlich dafür, wer für Schäden haftet, die einem Empfänger/Kunden durch den Zustelldienst schuldhaft zugefügt werden, und auf Basis welcher Rechtsgrundlage. Da nur die *Zustellspezifischen Leistungen* als Teilschritte des Hoheitsaktes angesehen werden können, handelt der Zustelldienst auch nur bei deren Ausführung als Organ der Behörde (§ 4 ZustG). Für Leistungen, welche ein Zustelldienst als Organ der Behörde erbringt,

kommen somit die Regelungen des AHG zur Anwendung. Die Allgemeinen Leistungen werden jedoch unabhängig von einem Zustellvorgang erbracht und können somit auch keiner Behörde zugerechnet werden. Der Ersatz von Schäden, welche im Zuge der Erbringung solcher Leistungen schuldhaft verursacht werden, sind folglich gemäß den Regelungen des allgemeinen Zivilrechts (§§ 1295 ff ABGB) vom Zustelldienst zu ersetzen.

3.3.4 Kontrahierungszwang

§ 29 Abs 6 ZustG sieht vor, dass der Zustelldienst bezüglich des Abschlusses von Verträgen über die Erbringung der Zustellleistung einem Kontrahierungszwang unterliegt.[87] Bezüglich der Herkunft (also der absendenden Behörde) zuzustellender Dokumente besteht der Kontrahierungszwang uneingeschränkt (Abs 6 aE). Möchte eine Behörde somit elektronische Zustellungen durchführen, so darf ihr dies vom Zustelldienst nicht verweigert werden. Bezüglich bestimmter Personengruppen von Empfängern steht es dem Zustelldienst jedoch frei, Einschränkungen zu treffen. Der Zustelldienst darf seine Leistung somit inhaltlich in der Form einschränken, dass er das Leistungsangebot (eigentlich die invitatio ad offerendum) auf die Zustellung an Personen bestimmter Personengruppen reduziert. Diese Einschränkung ist jedoch nur für bestimmte Personengruppen als Ganzes zulässig, für jede einzelne Person, welche einer solchen Personengruppe zuzuordnen ist, besteht wieder Kontrahierungszwang. Unabhängig davon, ob man der Ansicht folgt, dass der Vertrag über die Zustellleistung zwischen Behörde und Zustelldienst oder Kunde und Zustelldienst zu begründen ist, lässt sich die Formulierung des Abs 6 für beide Fälle anwenden. Da der Zustelldienst gegenüber Personen nicht bedienter Personengruppen keine der Teilleistungen des § 29 Abs 1 ZustG (auch nicht die *Allgemeinen Leistungen*) erbringen muss, kann solchen Personen gegenüber bereits die Durchführung einer Anmeldung gem § 33 ZustG verweigert werden.

Darüber hinaus ist der Vertrag zu den „üblichen Bedingungen mit jedermann“[88] zu schließen. Als übliche Bedingungen sind die mit der Zulassung genehmigten AGB sowie die Höhe des Entgelts für die Erbringung der Zustellleistung entsprechend dem Ausschreibungsvertrag gem § 32 Abs 1 ZustG zwischen BK und EuZD anzusehen.

---

[87] Vgl Erl zur RV 294 BlgNR 23. GP, 21.
[88] *Koziol/Welser/Kletecka*, Bürgerliches Recht I, 141.

3.4 Die Möglichkeit weitergehender zivilrechtlicher Vereinbarungen

Zu betonen ist in diesem Zusammenhang jedoch, dass nicht zu bestreiten ist, dass neben der Erbringung der Zustellleistung sehr wohl zivilrechtliche Vereinbarungen zwischen Kunde und Zustelldienst für die Erbringung von weitergehenden Dienstleistungen möglich sind. Das Zustellgesetz bietet hierfür auch unmissverständlich Anhaltspunkte (vgl §§ 29 Abs 3, 35 Abs 4 lS ZustG). Solche Leistungen werden jedoch nicht auf Grundlage des ZustG sondern des allgemeinen Zivilrechts erbracht. Sollen beispielsweise zugestellte Dokumente nach Ablauf der Speicherfrist weiterhin vom Zustelldienst gespeichert werden[89], so ist dies nichts Anderes als eine zivilrechtliche Vereinbarung über die Erbringung einer Hosting-Dienstleistung gem § 16 ECG. Detaillierte Ausführungen finden sich in Kapitel 11.

4. Die Anmeldung bei einem elektronischen Zustelldienst

Damit ein potentieller Empfänger von Ausfertigungen diese in elektronischer Form zugestellt bekommen kann, ist die Anmeldung bei einem zugelassenen Zustelldienst notwendig. Bei welchem konkreten Zustelldienst sich ein Kunde anmelden möchte, steht in dessen freiem Ermessen. Auf Grund des Grundsatzes der Wahlfreiheit des Kommunikationskanals zwischen Bürger und Behörde ist jedoch kein Bürger verpflichtet, sich bei einem Zustelldienst anzumelden.[90] Die Anmeldung bildet jedoch die öffentlich-rechtliche Willenserklärung, in die elektronische Zustellung von behördlichen Dokumenten einzuwilligen (§ 1 Abs 1 lS E-GovG, vgl Kapitel 3.2.4).

Den Rechtsrahmen für eine solche Anmeldung bildet § 33 ZustG. Dieser regelt, wie der konkrete Ablauf des Anmeldeprozesses zu erfolgen hat und welche Voraussetzungen dafür notwendig sind. Darüber hinaus ist genau festgelegt, welche Daten dem gewählten Zustelldienst bekannt zu geben sind. Weiters regelt § 33 jene Fälle, in welchen sich die Kundendaten geändert haben (Abs 2) oder sich ein Kunde vom Zustelldienst abmelden möchte (Abs 3).

4.1 Die technischen Voraussetzungen für die Anmeldung

§ 33 Abs 1 ZustG sieht vor, dass jeder Zustelldienst ein elektronisches Verfahren bereitstellen muss, welches eine Anmeldung beim Zustelldienst ermöglicht. Dies bedeutet de facto, dass die Möglichkeit einer Anmeldung durch Übermittlung

[89] § 35 Abs 4 lS ZustG.
[90] *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 381.

physischer Dokumente (wie zB ausgefüllter Formulare) gesetzlich ausgeschlossen ist. Diese Regelung hat jedoch lediglich klarstellenden Charakter, da sich das Erfordernis der Bereitstellung eines elektronischen Verfahrens bereits aus der verpflichtenden Verwendung der „Bürgerkarte“ (§ 2 Z 10 E-GovG) ergibt, welche notwendigerweise immer einer entsprechenden technischen Umgebung bedarf.

Das Gesetz trifft weiters genaue Regelungen, welche personenbezogenen Daten nach erfolgreicher Anmeldung vom Zustelldienst gespeichert werden müssen bzw. dürfen (§ 33 Abs 1 ZustG):

- Name bzw. Bezeichnung des Kunden
- bei natürlichen Personen das Geburtsdatum
- die zur eindeutigen Identifikation des Kunden im Bereich „Zustellwesen“ erforderlichen Daten:
    - bei natürlichen Personen das bereichsspezifische Personenkennzeichen (bPK) (§ 9 E-GovG)
    - sonst die Stammzahl (§ 6 E-GovG)
- genau eine elektronische Adresse, an die elektronische Verständigungen gemäß § 35 Abs 1 und 2 erster Satz ZustG übermittelt werden können
- gegebenenfalls (genau) eine inländische Abgabestelle, an die physische Verständigungen gemäß § 35 Abs 2 ZustG übermittelt werden können
- Angaben des Kunden darüber, welche Formate die zuzustellenden Dokumente aufweisen dürfen, damit er zu ihrer Annahme bereit ist
- Angaben des Kunden, die für eine allfällige inhaltliche Verschlüsselung der zuzustellenden Dokumente erforderlich sind.

Ein Kunde kann mit dem Zustelldienst jedoch auch vertraglich als weitere Leistung vereinbaren, dass Verständigungen an mehrere elektronische Adressen oder physische Abgabestellen übermittelt werden müssen (§ 33 Abs 1 lS ZustG)[91]. Dabei handelt es sich um eine zivilrechtliche Vereinbarung iSd § 29 Abs 3 ZustG, die über den Leistungsumfang der Zustellleistung gemäß dem ZustG hinausgeht und vom Zustelldienst ausschließlich auf Grund der vertraglichen Vereinbarung mit dem

[91] Erl zur RV 294 BlgNR 23. GP, 21.

Kunden zu erbringen ist. Dennoch ist diese vertragliche Vereinbarung für den Eintritt der Zustellwirkung relevant: Wurden mehrere elektronische Adressen oder physische Abgabestellen vom Kunden bekannt gegeben, so muss jede Verständigung jeweils an alle Adressen oder Abgabestellen übermittelt werden (§ 35 Abs 1 3. Satz 1. Halbsatz, § 35 Abs 2 aE ZustG). Der Zustelldienst kann sich somit nicht eine davon aussuchen. Weiters hat dies auch Auswirkungen auf den Fristenlauf, wobei § 35 Abs 8 ZustG auf diesen Umstand bezüglich des Eintritts der Zustellwirkung Rücksicht nimmt.

4.1.1 Name bzw Bezeichnung

Da als Kunden eines Zustelldienstes sowohl natürliche als auch juristische Personen in Betracht kommen, ist vom Zustelldienst entweder der Name einer natürlichen Person (Nachname und Vorname[n]) oder die Bezeichnung einer juristischen Person (zB Firma, Vereinsname, Behördenbezeichnung, etc) zu speichern.

4.1.2 Das bereichsspezifische Personenkennzeichen

Abhängig davon, ob sich eine natürliche oder juristische Person (vertreten durch eine vertretungsbefugte natürliche Person) beim Zustelldienst anmeldet, wird vom Zustelldienst im ersten Fall das bereichsspezifische Personenkennzeichen (bPK) für den staatlichen Tätigkeitsbereich *Zustellung* generiert und gespeichert (§ 9 E-GovG) bzw im zweiten Fall die Stammzahl (§ 6 E-GovG) der juristischen Person unverändert gespeichert. Dadurch kann jeder Kunde vom Zustelldienst Österreich weit eindeutig identifiziert werden (§ 2 Z 2 E-GovG). Verwechslungen oder Falschzustellungen sind daher ausgeschlossen. Gemäß Anlage 1 der E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV)[92] bildet „ZU“ die Bereichskennung für den staatlichen Tätigkeitsbereich *Zustellung*.

Da eine Anmeldung bei einem Zustelldienst ausschließlich unter Verwendung der Bürgerkarte erfolgen darf (§ 33 Abs 1 ZustG), steht dem Zustelldienst die Stammzahl bzw das bPK ohnedies zur Verfügung bzw kann entsprechend einem spezifizierten Algorithmus einfach berechnet werden. Weitere Erläuterungen zu diesen Personenkennzeichen und deren Berechnung erfolgen in Kapitel 5.

[92] BGBl II 289/2004.

4.1.3 Die elektronische Verständigungsadresse

Die elektronische Verständigungsadresse ist jene Kontaktinformation, welche der Kunde im Zuge seiner Anmeldung dem Zustelldienst bekannt gegeben hat, um an dieser Verständigungsadresse über das Vorliegen abholbereiter Zustellstücke informiert zu werden. Bei einer solchen Kontaktadresse kann es sich um beliebige Kommunikationskanäle handeln, wie zB E-Mail-Adressen, Telefonnummern für eine Verständigung per SMS, Skype-Adressen, MSN-Adressen, ICQ-Nummern, etc.[93] Bei solchen Verständigungsadressen sollte es sich um Kontaktmöglichkeiten zum Kunden handeln, bei welchen praktisch mit einer zeitnahen und sehr wahrscheinlichen Kenntnisnahme der Verständigung gerechnet werden kann.

Eine Verständigung an eine elektronische Kontaktadresse hat jedenfalls folgende Angaben zu beinhalten (§ 35 Abs 1 ZustG):

1. das Datum der Versendung
2. die Internetadresse, unter der das zuzustellende Dokument zur Abholung bereitliegt (praktisch derzeit die URL des Zustelldienstes)
3. das Ende der Abholfrist
4. einen Hinweis auf das Erfordernis einer Signierung bei der Abholung
5. einen Hinweis auf den Zeitpunkt, mit dem die Zustellung wirksam wird.

Wie eine solche Verständigung genau gestaltet sein muss, wird in der Zustellformularverordnung[94] (ZFormV) mit den Formularen 7 bis 9 geregelt. Soll eine Zustellung zu eigenen Handen erfolgen und hat der Kunde dem Zustelldienst eine physische Abgabestelle bekannt gegeben, so ist zur Verständigung Formular 7 zu verwenden ansonsten Formular 8. Für die (dritte) physische Verständigung ist Formular 9 zu verwenden (§ 3a ZFormV). Die Verordnungsermächtigung findet sich in § 35 Abs 1 lS ZustG.

Durch das Konzept der elektronischen Verständigungsadresse wird die Zustellleistung für den Kunden von einem Pull-Dienst in einen Push-Dienst übergeführt, was für diesen erhebliche Annehmlichkeiten mit sich bringt: Ein Kunde muss sein elektronisches Postfach beim Zustelldienst nicht in regelmäßigen Intervallen selbst darauf prüfen, ob eventuell Zustellstücke für ihn bereit liegen (Pull-

[93] Vgl Erl zur RV 252 BlgNR 22. GP, 14.
[94] BGBl II 600/1982 idF BGBl II 152/2008.

Dienst), sondern er wird aktiv erst dann vom Vorliegen eines Zustellstücks informiert, wenn tatsächlich ein solches zur Abholung bereit liegt (Push-Dienst).

4.1.4 Die physische Abgabestelle

Der Kunde kann im Zuge der Anmeldung beim Zustelldienst auch eine (physische) inländische Abgabestelle angeben. Diese Angabe ist zwar fakultativ (arg „gegebenenfalls“), hat jedoch Auswirkungen auf die Art und Anzahl der gesetzlich vorgeschriebenen Verständigungen über die Bereithaltung eines Dokuments beim elektronischen Zustelldienst und auch auf den Zeitpunkt des Eintritts der Zustellwirkung (vgl § 35 Abs 6 und 7 ZustG).

§ 2 Z 4 versteht unter einer Abgabestelle die „*Wohnung oder sonstige Unterkunft, die Betriebsstätte, der Sitz, der Geschäftsraum, die Kanzlei oder auch der Arbeitsplatz des Empfängers, im Falle einer Zustellung anlässlich einer Amtshandlung auch deren Ort, oder ein vom Empfänger der Behörde für die Zustellung in einem laufenden Verfahren angegebener Ort“.* Die Abgabestelle ist somit mit jener Örtlichkeit identisch, an welcher Dokumente im Zuge einer „herkömmlichen“ physischen Zustellung (§§ 13 ff ZustG) zugestellt werden können. Anders als bei der physischen Zustellung eines Dokuments stellt eine solche physische Verständigung jedoch keine Zustellung dar, sondern hat lediglich Auswirkungen auf den Zeitpunkt des Eintritts der Zustellwirkung. Hinsichtlich einer detaillierten Beschreibung, welche Örtlichkeiten konkret unter „Abgabestelle“ zu verstehen sind, kann auf die Literatur[95] verwiesen werden.

Die Verwendung der Legaldefinition „Abgabestelle“ im Zuge dieser Regelung erscheint auf den ersten Blick nahe liegend und relativ schlüssig, wirft im Detail jedoch eine Reihe von Fragestellungen bzw Problemen auf: Der Begriff der Abgabestelle ist im Gesetz durch die Legaldefinition des § 2 Z 4 ZustG genau festgelegt und wurde von der Judikatur weitgehend konkretisiert. Eine Frage, die sich somit in diesem Zusammenhang stellt, ist jene, welche Rechtsfolgen sich ergeben, wenn beispielsweise ein Kunde dem Zustelldienst gegenüber eine „Abgabestelle“ angibt, welche nicht von der Legaldefinition des ZustG umfasst ist (zB wenn sich jemand häufig auf Geschäftsreisen befindet und somit – um dennoch mit hoher Wahrscheinlichkeit über die Bereithaltung eines elektronischen Dokuments informiert

[95] Vgl *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 362 ff; *Hengstschläger*, Verwaltungsverfahrensrecht, 138 f.

zu werden – als Abgabestelle die Wohnung seiner Freundin angibt, ohne selbst dort wohnhaft zu sein oder Unterkunft zu haben). Auch eine Subsumtion unter sonstiger „angegebener Ort“ (§ 2 Z 7 letzter Fall) scheidet aus, da a) diese Angabe nicht gegenüber der Behörde sondern gegenüber dem Zustelldienst gemacht wird[96] und b) eine solche Angabe nicht notwendigerweise im Zuge eines laufenden Verfahrens gemacht werden muss.[97]

Für den Fall einer schriftlichen Verständigung an einer Abgabestelle über das Bereitliegen eines elektronischen Dokuments iSd § 33 Abs 1 Z 5 iVm 2 Z 4 ZustG wird die Legaldefinition „Abgabestelle“ in der Hinsicht wohl extensiv zu interpretieren sein, dass darunter jeder Ort zu verstehen sein wird, den der Kunde dem Zustelldienst für den Empfang physischer Verständigungen bekannt gegeben hat. Dies ist im Zuge einer teleologischen Interpretation damit zu begründen, dass Sinn und Zweck dieser fakultativen dritten Verständigung ein zusätzlicher Mechanismus zur Sicherstellung ist, dass ein Empfänger von der Bereithaltung elektronischer Dokumente auch dann tatsächlich Kenntnis erlangt, wenn diesem die elektronischen Verständigungen nicht zur Kenntnis gelangten. Weiters hat die strenge taxative Aufzählung, welche Örtlichkeiten als Abgabestelle dienen können, ihren Sinn und Zweck darin, dass ein Empfänger nur an bestimmten Orten mit (physischen) Zustellungen rechnen muss, die in der Regel auch ihn betreffende Rechtswirkungen entfalten. Diese gesetzliche Einschränkung auf lediglich bestimmte Örtlichkeiten, an welchen Zustellungen erfolgen dürfen, stellt für den Empfänger somit eine Schutzbestimmung dar.

Anders stellt sich dies im Falle einer physischen Verständigung im Zuge einer elektronischen Zustellung dar, da diese (abgesehen von bestimmten Fristen) an sich keine Rechtswirkungen entfaltet, sondern lediglich eine Information darstellt. Nimmt ein Kunde durch Bekanntgabe einer „Abgabestelle“ die Möglichkeit einer dritten (physischen) Verständigung in Anspruch, so stellt dies für ihn ein Mehr an Sicherheit dar, da ohne Angabe einer solchen Abgabestelle die Rechtswirkungen der Zustellung bereits auf Grund der elektronischen Verständigungen eintreten können.

[96] Das Zustellgesetz unterscheidet im Rahmen der physischen Zustellung sehr streng, ob bestimmte Angaben der Behörde oder dem Zustelldienst gegenüber gemacht werden. § 13 Abs 2 regelt die Bekanntgabe einer Empfangsbevollmächtigung gegenüber dem zustellenden Organ. Auch § 13 Abs 4 unterscheidet, ob der Ausschluss eines Mitarbeiters einer Kanzlei dem Zustellorgan (Satz 2) oder der Behörde (Satz 3) gegenüber bekannt gemacht wurde. Ähnlich stellt sich auch § 16 hinsichtlich der Ersatzzustellung dar (vgl Abs 3 und 4).

[97] Eine Anmeldung bei einem Zustelldienst kann jederzeit und unabhängig von behördlichen Verfahren oder sonstigen Aktivitäten durchgeführt werden.

Dass einem Empfänger die Möglichkeit einer dritten physischen Verständigung verwehrt bleiben soll, nur weil jener Ort, an welchem er diese Verständigung gerne erhalten möchte, keine „Abgabestelle“ iSd ZustG ist, ist nicht nachvollziehbar.

Zusammenfassend kann festgestellt werden, dass die Verwendung der Legaldefinition „Abgabestelle“ in den §§ 33, 35 und 36 ZustG wenig glücklich ist und einer konsequenten Rechtsanwendung nicht unbedingt zuträglich ist. Die alternative Verwendung des Begriffs „Ort“ wie in der Legaldefinition des § 2 Z 4 selbst (jedoch ohne weitere Einschränkungen) würde an dieser Stelle zu erheblicher Rechtssicherheit führen und auch eine konsequente Regelung darstellen.

4.1.5 Akzeptierte Dokumentenformate

Der Kunde muss dem Zustelldienst bei seiner Anmeldung all jene Dateiformate bekannt geben, die er zu empfangen bereit und zu lesen in der Lage ist. Die Notwendigkeit dieser Bekanntgabe ergibt sich daraus, dass ein Kunde im Vorhinein nicht wissen kann, welche Software in all jenen Behörden, die in Zukunft elektronische Dokumente zustellen werden, zum Einsatz kommt. Die Entscheidung, welche Software eine Behörde zur Erstellung von Bescheiden einsetzt, bleibt dieser auf Grund der innerbehördlichen Organisationshoheit selbst überlassen. Bis dato gibt es auch keine gesetzliche Vorschrift oder interbehördliche Vereinbarung, welche konkreten Dateiformate behördliche Ausfertigungen in elektronischer Form aufweisen müssen.[98] Dieses Problem stellt sich bei der physischen Zustellung logischerweise nicht, da bei dieser die Dokumente ausgedruckt und somit in einer für den Menschen lesbaren Form zugestellt werden.

Üblicherweise wird im Zuge der Anmeldung beim Zustelldienst eine Liste an möglichen Dateiformaten zur Verfügung gestellt, aus welchen die entsprechenden gewünschten Formate durch Selektion ausgewählt werden können. Diese Angaben können in späterer Folge (zB über das Webportal des Zustelldienstes) wieder geändert werden (§ 33 Abs 2 ZustG).

Die Behörde ihrerseits hat vor der Verfügung einer elektronischen Zustellung im Zuge der Abfrage beim Zustellkopf zu prüfen, welche Dateiformate der Empfänger in elektronischer Form zu empfangen bereit ist. Kann die Behörde auf Grund ihrer vorhandenen technischen Infrastruktur das zuzustellende Dokument nicht in diesem

[98] Nicht zu leugnen ist jedoch, dass sich die Dateiformate DOC(X) und PDF de facto zum Standard für Dokumente entwickelt haben.

Dateiformat erstellen, so muss eine elektronische Zustellung unterbleiben und das Dokument ist physisch zuzustellen. Dies kann entweder dadurch erfolgen, dass die Behörde nach der Kenntnisnahme, dass sie das von einem Empfänger angegebene Dateiformat nicht zu erstellen in der Lage ist, eine erneute Zustellverfügung erlässt oder dass die Zustellverfügung als Eventualanordnung ergeht (vgl Kapitel 1.4).

Die Angabe der akzeptierten Dateiformate aus technischer Sicht

Technisch werden zur Repräsentation der jeweils angegebenen Dateiformate die entsprechenden MIME-Types (Multipurpose Internet Mail Extensions)[99] verwendet. Dabei handelt es sich eigentlich um einen Standard, mit welchem bestimmte (binäre) Daten als Anhänge in E-Mails verschickt werden können. Da mit dem E-Mail-Protokoll SMTP (Simple Mail Transfer Protocol) lediglich Text als Messagebody versendet werden kann, wird mit den entsprechenden MIME-Types innerhalb des „Textkörpers“ angezeigt, dass es sich bei den nachfolgenden Zeichen um (codierte) binäre Daten in einem bestimmten Datenformat handelt. Damit kann die Mailclientsoftware erkennen, mit welcher Applikation die so eingebetteten „Anhänge“ zu öffnen sind. Diese MIME-Types kommen – wenn auch relativ zweckentfremdet – in diesem Zusammenhang zur Anwendung.

MIME-Types werden immer mit Datentyp und konkretem Dateiformat mit Schrägstrich getrennt angegeben.

Syntax: `<Datentyp>/<Datenformat> (type/subtype)`

Beispiele: `text/txt, text/xml, text/html, application/msword, application/pdf, image/gif`

4.1.6 Angaben zur inhaltlichen Verschlüsselung

Ein Kunde kann dem Zustelldienst „Angaben“ übermitteln, mit welchen die Behörde die zuzustellenden Dokumente vor Übermittlung an den Zustelldienst verschlüsseln muss. Es steht dem Kunden frei, ob er eine solche inhaltliche Verschlüsselung wünscht oder nicht (arg „allfällige“). Hat eine Kunde solche „Angaben“ bei seinem Zustelldienst hinterlegt, so sind diese dem Zustellkopf ebenfalls zu übermitteln. Möchte nun eine Behörde an einen bestimmten Empfänger elektronisch zustellen, so muss im Zuge der Zustellkopfabfrage auch ermittelt werden, ob der Empfänger

[99] RFCs 2045 - 2049.

solche Angaben hinterlegt hat. Ist dies der Fall, so MUSS die Behörde die zuzustellenden Dokumente zuvor verschlüsseln, bevor sie diese an den Zustelldienst zur Durchführung der Zustellung übergeben darf. Ist sie dazu nicht in der Lage, muss eine physische Zustellung verfügt werden.

Bereitstellung einer vertraulichen Ende-zu-Ende-Kommunikation

Mit dieser technischen Konzeption wurde die Möglichkeit einer sicheren und vertraulichen Ende-zu-Ende-Kommunikation zwischen Behörde und Empfänger geschaffen. Bereits bevor zuzustellende Dokumente an einen Zustelldienst übergeben werden, müssen diese Dokumente direkt von der zustellenden Behörde mit den „Angaben“ des Kunden verschlüsselt werden. Nur der Empfänger selbst kann die Dokumente wieder entschlüsseln, wodurch deren Vertraulichkeit auf dem gesamten Übertragungsweg zwischen Behörde und Empfänger sichergestellt werden kann. Auch dem Zustelldienst (respektive dessen Mitarbeitern) ist es zu keinem Zeitpunkt möglich, den Inhalt der zuzustellenden Dokumente zu lesen. Daraus ergibt sich, dass ein Dokument auf seinem Weg zwischen Sender und Empfänger von niemandem eingesehen werden kann („Ende-zu-Ende-Kommunikation“).

Verpflichtung zur Verschlüsselung

Möchte nun eine Behörde an einen Empfänger zustellen, der Angaben zur inhaltlichen Verschlüsselung hinterlegt hat, so sind grundsätzlich 2 Fälle zu unterscheiden:

a) Hinterlegung von Verschlüsselungsdaten bei allen Zustelldiensten

Dieser Fall, in welchem der Empfänger bei einem oder mehreren Zustelldiensten angemeldet ist und bei jedem dieser Zustelldienste Angaben zur Verschlüsselung hinterlegt hat, kann die Behörde nach eigenem Ermessen einen Zustelldienst frei wählen.[100] Sie muss die zuzustellenden Dokumente jedoch mit den entsprechenden beim gewählten Zustelldienst hinterlegten Verschlüsselungsangaben verschlüsseln.

b) Hinterlegung von Verschlüsselungsdaten bei einigen Zustelldiensten

Der zweite Fall, in welchem der Empfänger bei mehreren Zustelldiensten angemeldet ist aber nur bei einigen davon Verschlüsselungsangaben hinterlegt hat, stellt sich rechtlich nicht ganz so unzweifelhaft dar. Für diesen Fall sieht § 34 Abs 3 ZustG zwar

[100] *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 383.

die klare Regelung vor, dass bei der möglichen Auswahl aus mehreren Zustelldiensten, bei welchen der Empfänger registriert ist, die Behörde jenem den Vorzug zu geben hat, bei welchem Angaben zur inhaltlichen Verschlüsselung hinterlegt sind. Jedoch stellt sich in einer solchen Konstellation aber die Frage, ob die Behörde, wenn sie nicht über die technischen Möglichkeiten einer Verschlüsselung verfügt, über einen jener Zustelldienste zustellen darf, bei welchen keine Verschlüsselungsangaben hinterlegt wurden oder ob in einem solchen Fall die elektronische Zustellung gänzlich unterbleiben muss.

Grundsätzlich muss sich diese Frage nach den Vorstellungen des Empfängers richten, welcher sich auf Grund seiner Wahlfreiheit gem § 1 Abs 1 E-GovG dafür entschieden hat, dass die Behörde auch mittels eines elektronischen Kommunikationskanals – hier in Form der elektronischen Zustellung – an ihn herantreten darf (vgl Kapitel 3.2.4). Ist bzw bleibt ein solcher Empfänger bei einem elektronischen Zustelldienst angemeldet, ohne bei diesem Angaben zur inhaltlichen Verschlüsselung zu hinterlegen, obwohl er dies bei anderen Zustelldiensten, bei welchen er ebenfalls angemeldet ist bzw bleibt, getan hat, so wird man davon ausgehen dürfen, dass er lieber einer unverschlüsselten Zustellung den Vorzug gibt, als Dokumente gänzlich physisch zugestellt zu bekommen. Sollte dies nicht in seinem Interesse liegen, so stellt sich die Frage, warum der Empfänger weiterhin bei einem Zustelldienst angemeldet bleibt bzw warum er in einem solchen Fall auch bei dem oder den weiteren Zustelldienst(en) keine Verschlüsselungsangaben hinterlegt.

Weitere Argumente für die erste Variante sind der Wortlaut des Gesetzes und die mangelnde praktische Sinnhaftigkeit der zweiten Variante. Dem Wortlaut des § 34 Abs 3 ZustG zufolge ist „*bei Auswahl zwischen mehreren in Betracht kommenden Zustelldiensten*„ eben *„jenem der Vorzug zu geben“*, was auf die Notwendigkeit des Vorliegens einer gewissen Wahlfreiheit seitens der Behörde schließen lässt. Eine solche Wahlfreiheit ist jedoch nicht gegeben, wenn die Behörde technisch gar nicht in der Lage ist, die Dokumente vor deren Zustellung zu verschlüsseln, wodurch ein Zustelldienst, bei welchem Verschlüsselungsangaben hinterlegt sind, aus Sicht der Behörde eben nicht für eine Zustellung in Betracht kommen kann. Zweitens würde diese Regelung im Verständnis der zweiten Variante dazu führen, dass keine Behörde mehr über jenen Zustelldienst zustellen dürfte, bei welchem keine Verschlüsselungsangaben hinterlegt sind, was zur Frage der Sinnhaftigkeit führt, warum ein Empfänger bei einem solchen angemeldet bleiben sollte. Aus diesem

Grund kann einem solchen Empfänger nicht der Wille unterstellt werden, dass er – obwohl er bei einem elektronischen Zustelldienst ohne Hinterlegung von Verschlüsselungsangaben angemeldet bleibt – lieber physische Zustellungen empfangen möchte, wenn der Behörde aus technischen Gründen keine Verschlüsselung möglich ist. Diese Ansicht entspricht auch der alten Fassung des § 33 ZustG idF BGBl I 10/2004: *Verfügt die Behörde daraufhin die elektronische Zustellung, ist das Dokument, wenn möglich in verschlüsselter Form, dem zuständigen Zustelldienst zur weiteren Veranlassung zu übergeben.*

„Angaben" zur inhaltlichen Verschlüsselung

Einer näheren Konkretisierung bedarf an dieser Stelle auch der vom Zustellgesetz verwendete Begriff der „Angaben zur inhaltlichen Verschlüsselung". Prinzipiell basiert die Verschlüsselung im gesamten Zustellsystem auf asymmetrischen Verschlüsselungsverfahren. Bei diesem Verfahren kommen zwei verschiedene Schlüssel zum Einsatz, nämlich der „Private Schlüssel" und der „Öffentliche Schlüssel". Wie die Bezeichnung bereits vermuten lässt, darf der Private Schlüssel nur dem Inhaber bekannt sein und nicht an Dritte weitergegeben werden. Der Private Schlüssel muss somit vom Inhaber geheim gehalten werden, da ansonsten die Vertraulichkeit dieses Verfahrens nicht mehr gewährleistet sein würde. Der Öffentliche Schlüssel hingegen darf beliebig an Dritte weitergegeben werden bzw ist dies sogar praktisch notwendig, damit das Verschlüsselungsverfahren zum Einsatz kommen kann. Die beiden Schlüssel sind in der Form voneinander abhängig, dass Daten, die mit einem der beiden Schlüssel verschlüsselt wurden, ausschließlich mit dem jeweils anderen korrespondierenden Schlüssel wieder entschlüsselt werden können. Eine Entschlüsselung von Daten mit demselben Schlüssel, mit welchem auch die Verschlüsselung erfolgte, ist bei asymmetrischen Verfahren nicht möglich.

Die Vertraulichkeit der zu übermittelnden Daten kann mit diesem Verfahren folglich in der Form sichergestellt werden, dass der Absender die Daten mit dem Öffentlichen Schlüssel des Empfängers, der ja jedermann bekannt sein darf bzw auch bekannt sein soll, verschlüsselt. Somit kann nur der Empfänger, welcher ja einzig und allein über den korrespondierenden Privaten Schlüssel verfügt, die übermittelte Nachricht wieder entschlüsseln. Einem Dritten ist die Entschlüsselung somit nicht möglich.

Diese „Angaben" zur inhaltlichen Verschlüsselung iSd § 33 Abs 1 Z 7 sind somit eine Datei, welche ein digitales Zertifikat (vgl § 2 Z 8 SigG) enthält, das den Öffentlichen

Schlüssel des Empfängers und weitere Informationen über diesen beinhaltet (vgl Kapitel 5.3.4).

Möchte eine Behörde nun eine elektronische Zustellung an einen Empfänger vornehmen, so erhält sie im Zuge der Zustellkopfabfrage auch die entsprechenden bei den einzelnen Zustelldiensten hinterlegten Zertifikatsdateien. Im Anschluss muss auf Seite der Behörde das Zertifikat auf Gültigkeit geprüft, der Öffentliche Schlüssel des Empfängers aus der Zertifikatsdatei ausgelesen und die zuzustellenden Dokumente mit diesem verschlüsselt werden. Erst danach dürfen die Dokumente an den Zustelldienst zur Zustellung an den Empfänger übergeben werden.

4.2 Die Änderung von Kundendaten

Der Kunde ist verpflichtet, dem Zustelldienst Änderungen in seinen Kundendaten unverzüglich bekannt zu geben. Unter „unverzüglich“ wird ohne schuldhaftes Verzögern zu verstehen sein.[101]

Bei dieser Anordnung handelt es sich zwar um eine gesetzliche Verpflichtung, unmittelbare Rechtsfolgen (zB in Form von Geldbußen) sind an eine Unterlassung jedoch nicht geknüpft. Dennoch kann die Unterlassung der Aktualisierung für einen Empfänger unangenehme Folgen haben, indem beispielsweise zugestellte Dokumente Zustellwirkung entfalten können, von denen er entweder gar keine Kenntnis hatte oder deren Inhalt er technisch bedingt nicht (mehr) lesen kann. Dies könnte sich beispielsweise dadurch ereignen, dass eine Behörde verschlüsselte Dokumente zustellt, die entsprechenden Entschlüsselungsdaten beim Empfänger jedoch nicht mehr vorhanden sind (zB Arbeitsplatzwechsel, Neuerwerb eines Computers, Defekt eines Datenträgers etc).

§ 33 Abs 2 ist in Bezug auf § 8 ZustG als lex specialis zu sehen, weswegen § 8 für die Änderung einer Abgabestelle im Kontext der elektronischen Zustellung nicht zur Anwendung kommt.[102] Folglich kann jedoch festgestellt werden, dass die Regelung des § 8 ZustG im 2. Abschnitt des ZustG aus systematischer Sicht besser aufgehoben wäre.

[101] Vgl *Feil*, Zustellwesen, 38, mwN.
[102] Vgl *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 382.

4.3 Die Bekanntgabe von Abwesenheitszeiten

Bei einem Zustelldienst angemeldete Personen sind berechtigt, diesem bestimmte Zeiträume bekannt zu geben, innerhalb welcher sie einer elektronischen Zustellung von Dokumenten nicht zustimmen. Für solche Zeiträume gilt die Einwilligung in den Erhalt elektronischer Zustellungen gem § 1 Abs 1 E-GovG als zurückgezogen. Diese Abwesenheitsmeldung erspart dem potentiellen Empfänger die Abmeldung bei Beginn und erneute Anmeldung beim Zustelldienst nach Ablauf eines solchen „Abwesenheitszeitraums“. In einem solchen Fall kann jedoch auf die physische Zustellung zurückgegriffen werden, wobei auch hier die Regelungen zur Abwesenheit von der Abgabestelle zu berücksichtigen sind.

4.4 Der technische Ablauf einer Anmeldung

Grundsätzlich hat jeder Zustelldienst ein elektronisches Verfahren zur Anmeldung bereit zu stellen (§ 33 Abs 1 2. Satz ZustG). Wie dieses Verfahren technisch konkret ausgestaltet ist, liegt im freien Ermessen des Zustelldienstes. Die technische Lösung muss lediglich die Anforderungen des Bürgerkartenkonzepts gem §§ 2 Z 10 iVm 4 ff E-Gov erfüllen.
In der Regel ruft ein potentieller Nutzer die Internetseite des gewünschten Zustelldienstes auf, wo sich die entsprechenden Informationen und technischen Möglichkeiten zur Durchführung der Anmeldung finden. Abhängig davon, über welche technischen Implementierungen bezüglich der Bürgerkartenumgebung der Zustelldienst verfügt, kann die Anmeldung unter Verwendung verschiedener Techniken erfolgen (zB lokale BKU oder online BKU, mit Signaturkarte unter Verwendung eines Kartenlesers, mobile BKU unter Verwendung eines Mobiltelefons, etc).

Im ersten Schritt wird der Benutzer zur Eingabe seiner PIN (bei Verwendung der Signaturkarte) oder seiner Anschlussnummer und seinem Passwort (bei Verwendung der mobilen Signatur) aufgefordert. Nachdem die Eingabe korrekt erfolgte (und ggf der an das Mobiltelefon übermittelte TAN eingegeben wurde), wird die Personenbindung aus der Bürgerkarte ausgelesen und das bPK für den Verwaltungsbereich *Zustellung* automatisch generiert (vgl Kapitel 5). Da die Personenbindung bereits Vorname, Nachname und Geburtsdatum beinhaltet, werden diese Daten in der Regel automatisch in die entsprechenden dafür vorgesehenen Eingabefelder übernommen und können auch nicht verändert werden. Dadurch wird die (Ver-)Fälschung von I-

dentitätsdaten verhindert. An dieser Stelle müssen auch alle weiteren von § 33 ZustG geforderten Daten eingegeben werden, fakultative Angaben können entweder bereits hier getätigt oder in späterer Folge über die Benutzeroberfläche nachgeholt werden. Weiters ist auch eine elektronische Adresse für Verständigungen anzugeben. Eine solche Adresse wird in der Regel durch Übermittlung eines Aktivierungslinks verifiziert. Erst nach Betätigung dieses Aktivierungslinks ist die Anmeldung gem § 33 ZustG abgeschlossen und das Zustellpostfach wird für Zustellungen frei geschaltet.

4.5 Der Ablauf einer Datenänderung und einer Abmeldung

Nach erfolgter Anmeldung muss dem Kunden vom Zustelldienst die Möglichkeit geboten werden, seine Kundendaten zu ändern, Abwesenheitszeiträume bekannt zu geben (vgl Kapitel 4.3) oder sich gänzlich vom Zustelldienst abzumelden.

Üblicherweise können Daten oder Abwesenheitszeiträume über die Benutzeroberfläche des Zustelldienstes administriert werden, jedoch ist dies nicht die technisch einzig mögliche Variante. Insbesondere § 33 Abs 2 ZustG gibt keine explizite Auskunft darüber, wie eine solche Datenadministration erfolgen muss. Allein dem Wortlaut entsprechend könnte diese auch durch Übermittlung physischer Schriftstücke erfolgen, da im Gegensatz zu Abs 1 die Notwendigkeit der Bereitstellung bzw Verwendung eines elektronischen Verfahrens nicht vorgeschrieben ist. In der Praxis hat sich derzeit die Verwendung von Eingabefeldern und Bestätigungsbuttons durchgesetzt. Weiters geht aus dieser Regelung nicht hervor, ob die geänderten Daten mit der Bürgerkarte digital signiert werden müssen oder ob die Betätigung eines Buttons ausreicht. Im Umkehrschluss zu Abs 1 und 3 wird zweites wohl zu bejahen sein. Dennoch sollte die erforderliche Bestätigung der neuen Daten mittels Bürgerkarte der Rechtssicherheit und Nachvollziehbarkeit halber angedacht werden, da eine digitale Signatur dem Diskriminierungsverbot im gerichtlichen Verfahren unterliegt (§ 3 SigG). Weiters normiert § 4 Abs 3 SigG: *„Die Bestimmung des § 294 ZPO über die Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde ist auf elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, anzuwenden“*. Besonders bei der „Änderung“ von Daten, die eigentlich die Abgabe einer Willenserklärung (wie beispielsweise die Einwilligung in die Zusendung von Dokumenten im Auftrag von Privaten gem § 29 Abs 3 ZustG) darstellt, bringt die Auf-

bringung einer digitalen Signatur wesentliche rechtliche und beweistechnische Vorteile.

Eine Abmeldung vom Zustelldienst und damit der Widerruf der Einwilligung in den Empfang von behördlichen Dokumenten mittels elektronischer Zustellung muss mittels Bürgerkarte oder durch schriftliche (physische) Erklärung an den Zustelldienst erfolgen. Die Abmeldung ist sofort mit Einlangen beim Zustelldienst wirksam. Die vertragliche Vereinbarung bestimmter „Kündigungsfristen“ in Bezug auf die behördliche Zustellung von Dokumenten ist somit nicht zulässig. Bei allen aktuell zugelassenen Zustelldiensten kann eine Abmeldung derzeit nur durch Klick auf einen Button „Postfach auflösen“ erfolgen, was folglich nicht den gesetzlichen Erfordernissen entspricht.

4.6 Die Übermittlung der Daten an den Zustellkopf

Gemäß § 29 Abs 1 Z 1 ZustG muss der Zustelldienst die Daten neu angemeldeter Kunden, geänderte Daten bestehender Kunden oder Abwesenheitsnotizen „unverzüglich“ an den EuZD weiterleiten, um den Zustellkopf als zentralen Verzeichnisdienst aller Personen, welche in die elektronische Zustellung behördlicher Dokumente eingewilligt haben, stets aktuell zu halten. Diese Leistung stellt die *Aktualisierungsleistung* dar, welche in Kapitel 6 einer näheren Beleuchtung unterzogen wird.

Widersprüchlicher Weise bezieht sich die Regelung des § 29 Abs 1 Z 1 ZustG lediglich auf die Absätze 1 und 2 des § 33 ZustG, nicht jedoch auf Abs 3. Dies würde streng dem Wortlaut zufolge bedeuten, dass dem Zustellkopf die Löschung von Daten auf Grund einer Abmeldung durch einen Kunden nicht mitzuteilen wären. Dabei kann es sich bei holistischer Betrachtungsweise des ZustG lediglich um eine planwidrige Lücke handeln, da es system- und zweckwidrig wäre, einen Kunden, der bei einem bestimmten Zustelldienst nicht mehr angemeldet ist, dennoch beim Zustellkopf evident zu halten. Daraus würde weiters folgen, dass die Richtigkeit der Ermittlungsleistung nicht mehr gewährleistet werden könnte und die Behörde möglicherweise eine Zustellverfügung für einen elektronischen Zustelldienst erlassen würde, bei welchem der Empfänger gar nicht mehr angemeldet ist. Diese planwidrige Lücke wird man somit mit Interpretation schließen dürfen und auch für den Fall einer Abmeldung die Pflicht zur unverzüglichen Ausführung der Aktualisierungsleistung annehmen

müssen.[103] Aus datenschutzrechtlicher Sicht ergibt sich gem § 6 DSG sogar eine Pflicht zur Löschung sowohl beim Zustelldienst als auch beim Zustellkopf, da nach Zweckerfüllung eine weitere Speicherung von Daten nicht mehr zulässig ist und diese folglich zu löschen sind. Eine Anpassung des Gesetzestextes zB in der Form, dass eine Litera d für diesen Fall eingefügt wird, wäre wünschenswert. Diese könnte beispielsweise lauten: „*d) der Information, dass sich ein Kunde gem § 33 Abs. 3 abgemeldet hat*".

5. Das Konzept der Bürgerkarte

§ 33 Abs 1 ZustG sieht vor, dass eine Anmeldung beim Zustelldienst ausschließlich (arg „nur") unter Verwendung der *„Bürgerkarte"* erfolgen kann. Auch die Abmeldung vom Zustelldienst kann mit der Bürgerkarte erfolgen, jedoch ist auch eine schriftliche Abmeldung möglich (§ 33 Abs 3 ZustG). Eine unabdingbare Voraussetzung für die Inanspruchnahme der elektronischen Zustellung ist somit, dass sich der (potentielle) Empfänger im Besitz einer Bürgerkarte befindet. Mit Hilfe der Bürgerkarte kann allgemein eine qualifizierte, nachvollziehbare und verbindliche Kommunikation zwischen zwei Akteuren sichergestellt werden. Dies ist notwendig, um sicherstellen zu können, dass das Dokument einerseits tatsächlich dem richtigen Empfänger ausgehändigt wird und andererseits beweisbar protokolliert werden kann, dass ein Dokument zu einem bestimmten Zeitpunkt tatsächlich in den Verfügungsbereich des Empfängers zugegangen ist.

5.1 Zweck und Nutzen der Bürgerkarte

Zweck der Bürgerkarte ist es, die Identität, Authentizität, Integrität und Verbindlichkeit einer Kommunikation zwischen zwei Parteien (insb zwischen Behörden und Bürgern) auch im Internet sicherstellen zu können.

5.1.1 Qualitätsvolle Kommunikation

Für eine qualitätsvolle Kommunikation, die den Anforderungen des ZustG (und auch jenen des E-GovG) entspricht, müssen folgende Aspekte sichergestellt sein:[104]

[103] Vgl in diesem Zusammenhang auch die Spezifikation ZUSEPUSH, die ebenfalls bei *jeglicher* Änderung von Daten bei einem Zustelldienst von der Pflicht zur Ausführung der Aktualisierungsleistung ausgeht (*Tauber*, ZUSEPUSH, 6).

[104] Vgl *Bitzer/Brisch*, Digitale Signatur; 2 ff.

Identität: Da nur an jenen Empfänger tatsächlich zugestellt werden darf, der in der Zustellverfügung gem § 5 ZustG von der Behörde bezeichnet wird, ist die Identität des Empfängers vor der tatsächlichen Übergabe des Dokuments festzustellen. In § 2 Z 1 E-GovG findet sich die Legaldefinition des Begriffs Identität: „*Bezeichnung der Nämlichkeit von Betroffenen durch Merkmale, die in besonderer Weise geeignet sind, ihre Unterscheidbarkeit von anderen zu ermöglichen; solche Merkmale sind insbesondere der Name, das Geburtsdatum und der Geburtsort, aber auch etwa die Firma oder (alpha)nummerische Bezeichnungen".* Vor allem bei Namensgleichheit zweier Personen an ein und derselben Abgabestelle[105] ist durch weitere Angaben in der Zustellverfügung sicherzustellen, dass das zuzustellende Dokument tatsächlich nur jener Person ausgehändigt wird, für welche es bestimmt ist. Dies kann beispielsweise durch weitere Angaben wie „Jun" oder "Sen" oder das Geburtsdatum erfolgen.

Authentizität: Authentizität bedeutet, dass das Dokument tatsächlich von der Person (respektive Behörde) stammt, welche vorgibt, der Urheber des zuzustellenden Dokuments zu sein. Durch Sicherstellung der Authentizität kann folglich gewährleistet werden, dass das Dokument tatsächlich vom ausgewiesenen Urheber stammt, also nicht *gefälscht* wurde. Auch für die Authentizität existiert eine Legaldefinition im E-GovG: „*Die Echtheit einer Willenserklärung oder Handlung in dem Sinn, dass der vorgebliche Urheber auch ihr tatsächlicher Urheber ist."* (§ 2 Z 5).

Integrität: Bei der Übermittlung eines Dokuments muss weiters sichergestellt werden, dass der Inhalt des Dokuments weder beim Versender noch auf dem Übertragungsweg *verfälscht* wurde bzw eine Verfälschung vom Empfänger zumindest verlässlich erkannt werden kann. Die Integrität bildet einen Teilaspekt der Authentizität, da eine nicht integere Nachricht in der Form nicht vom Urheber stammt und daher auch nicht authentisch ist.

Vertraulichkeit: Da in Kommunikationen mit Behörden (insbesondere bei der Zustellung behördlicher Dokumente) in der Regel personenbezogene Daten des Empfängers oder sonstiger Betroffener übermittelt werden, ist die Vertraulichkeit einer solchen Kommunikation sicherzustellen. Vertraulichkeit bedeutet, dass nur berechtigte

[105] § 2 Z 4 ZustG.

Personen vom Inhalt solcher Kommunikationen Kenntnis erlangen können, unberechtigte Dritte jedoch nicht.

Verbindlichkeit: Dieser Aspekt bedeutet, dass die Abgabe einer (elektronischen) Willenserklärung oder – wie im Bereich der Zustellung – deren Empfang bestimmte Rechtswirkungen auslöst. Das ZustG sieht detaillierte Formerfordernisse an die Zustellung behördlicher Dokumente vor, damit der Zugang dieses Dokuments auch entsprechende Rechtswirkungen entfaltet. Durch Sicherstellung der Verbindlichkeit ist jedem Kommunikationspartner klar, dass mit der gegenständlichen Kommunikation Rechtsfolgen verbunden sind.

Nichtabstreitbarkeit: Dieser Aspekt soll sicherstellen, dass die Abgabe einer Willenserklärung mit einem bestimmten Inhalt oder der Zugang einer solchen in späterer Folge weder vom Absender noch vom Empfänger bestritten werden können soll. Auch der Zeitpunkt der Abgabe oder des Zugangs der Erklärung soll dauerhaft nachvollziehbar sein. Die Nichtabstreitbarkeit ist vor allem dann von rechtlicher Relevanz, wenn an die Abgabe einer Willenserklärung bestimmte Rechtsfolgen geknüpft sind.

5.1.2 Qualifizierte Kommunikation im physischen Zustellverfahren

Im konventionellen (physischen) Zustellverfahren wird die qualifizierte Kommunikation durch verschiedene Formalitäten erfüllt: Die Identität und Authentizität des Absenders wird durch das Briefpapier der Behörde, die Unterschrift des Genehmigungsbefugten sowie die Aufbringung des Amtsstempels sichergestellt. Die Integrität wird durch Verwendung schwer manipulierbarer Ausfertigungsverfahren[106] gewährleistet, sowie die Vertraulichkeit durch Zustellung in einem Briefkuvert (ggf versehen mit einem Behördensiegel) und durch Beauftragung eines vertrauenswürdigen Zustellorgans iSd § 3 ZustG. Die Verbindlichkeit wird dadurch hergestellt, dass der Empfänger bzw ein Zustellbevollmächtigter[107] gegenüber dem Zustellorgan den Empfang durch Unterschrift unter Beisetzung des Datums quittieren muss. Somit kommt auch im physischen Zustellverfahren eine aus dem Bereich der Technik sehr bekannte Maßnahme zur Erhöhung der Sicherheit einer Kommunikation und erleichterten

[106] ZB Verwendung von Kugelschreiber statt Bleistift.
[107] §§ 9 f ZustG.

Beweisführung zum Einsatz: Die Hinzuziehung einer für beide Parteien *vertrauenswürdigen dritten Partei* („Trusted Third Party“).

5.1.3 Qualifizierung im elektronischen Zustellverfahren

Bei der elektronischen Zustellung müssen nun ebenfalls die für eine qualifizierte Kommunikation erforderlichen Anforderungen erfüllt werden. Dafür können im Internet nahe liegender Weise nicht dieselben Verfahren wie bei der herkömmlichen (physischen) Zustellung zur Anwendung kommen.

Zur Sicherstellung der Identität, Authentizität, Integrität, Verbindlichkeit und Nichtabstreitbarkeit kommt das Verfahren der **„Digitalen Signatur“** unter Hinzuziehung einer vertrauenswürdigen dritten Partei, dem Zertifizierungsdiensteanbieter (kurz ZDA), zum Einsatz. Eine digitale Signatur stellt (auf den konventionellen Bereich umgemünzt) eine Art Unterschrift unter einem bestimmten Text (ggf einschließlich Datum) dar, die einer ganz bestimmten Person zugeordnet werden kann. Der Nachweis, dass von einer bestimmten Person zu einem bestimmten Zeitpunkt eine Willenserklärung abgegeben oder empfangen wurde, kann entweder vom Absender, vom Empfänger oder gänzlich von einer vertrauenswürdigen dritten Partei je mit ihrer digitalen Signatur bestätigt werden.

Die Vertraulichkeit wird durch den Einsatz technologisch sicherer Verschlüsselungsverfahren gewährleistet, die zwar auf derselben Technologie wie die digitale Signatur basieren, dennoch auf gänzlich andere Art und Weise zum Einsatz kommen (vgl Kapitel 4.1.6).

5.1.4 Das Verfahren der digitalen Signatur

Die digitale Signatur ist ein Datensatz, der im Zuge der Signaturerstellung aus dem ursprünglichen Dokument abgeleitet (generiert) und vom Absender auf eine bestimmte Art und Weise verändert („verschlüsselt“) wird. Diese digitale Signatur wird in der Folge zusammen mit dem zuzustellenden Dokument an den Empfänger übermittelt.

Ausgangstechnologie: Analog zur Verschlüsselung ist auch für die Erstellung und Prüfung digitaler Signaturen das Asymmetrische Verschlüsselungsverfahren die Basistechnologie, welche bereits in Kapitel 4.1.6 erläutert wurde. Bei der digitalen Sig-

natur werden die beiden Schlüssel jedoch genau umgekehrt verwendet: der Private Schlüssel zum Verschlüsseln und der Öffentliche Schlüssel zum Entschlüsseln.

Signaturerstellung: Im ersten Schritt wird aus dem ursprünglichen Dokument in einem unumkehrbaren Einwegverfahren („Hash-Verfahren“) ein Datensatz bestimmter Länge („Hash-Wert“) generiert, der das Dokument repräsentativ (also wie eine Art Fingerabdruck) abbildet. Wird auch nur 1 Bit in der Quelldatenmenge verändert, ändert sich auch der Hash-Wert. Weiters ist es unmöglich, aus dem Hash-Wert das ursprüngliche Dokument zu rekonstruieren. Im zweiten Schritt wird dieser Hash-Wert mit dem Privaten Schlüssel des Absenders, der ja nur diesem bekannt sein darf, verschlüsselt. Eine Entschlüsselung dieses Hash-Wertes ist in der Folge nur mehr mit dem korrespondierenden Öffentlichen Schlüssel möglich. Der Empfänger muss aber wissen bzw sicher sein können, dass dieser Öffentliche Schlüssel tatsächlich dem entsprechenden Absender zugeordnet ist. Dies kann entweder dadurch sichergestellt werden, dass der Öffentliche Schlüssel dem Empfänger vom Sender persönlich (oder in einem anderen sicheren Verfahren) übergeben wurde, oder von einer vertrauenswürdigen dritten Partei bestätigt wird, dass dieser Öffentliche Schlüssel tatsächlich dem Absender zugeordnet ist. Der so verschlüsselte Hash-Wert stellt nun die „digitale Signatur“[108] des Dokuments dar.

Signaturprüfung: Um die Authentizität und Integrität eines erhaltenen Dokuments zu prüfen, muss der Empfänger die mit dem Dokument übermittelte digitale Signatur überprüfen. Dazu entschlüsselt er im ersten Schritt die empfangene digitale Signatur mit dem Öffentlichen Schlüssel des Absenders, von welchem er wissen muss, dass dieser tatsächlich dem Absender zugeordnet ist. Im zweiten Schritt erzeugt der Empfänger aus dem erhaltenen Dokument analog zum Signaturerstellungsvorgang ebenfalls den Hash-Wert und vergleicht diesen mit der entschlüsselten digitalen Signatur. Stimmen beide überein, so war die Prüfung erfolgreich und das Dokument ist authentisch und integer. Wurde auf dem Übertragungsweg jedoch nur ein Bit im Dokument verändert, ergibt sich beim Empfänger ein anderer Hash-Wert als jener, den die Entschlüsselung der digitalen Signatur lieferte. Dadurch ist für den Empfänger erkennbar, dass das Dokument am Übertragungsweg verändert wurde.

[108] Andere Bezeichnungen dafür sind auch „Signaturwert“ oder „Signaturdaten“.

5.2 Definition und Rechtsrahmen der Bürgerkarte

Die Legaldefinition des § 2 Z 10 E-GovG normiert unter dem Begriff „Bürgerkarte“ folgendes: „*eine logische Einheit, die unabhängig von ihrer technischen Umsetzung eine qualifizierte elektronische Signatur (§ 2 Z 3a SigG) mit einer Personenbindung (§ 4 Abs 2) und den zugehörigen Sicherheitsdaten und -funktionen sowie allenfalls mit Vollmachtsdaten verbindet“.*

Es handelt sich beim Begriff der „Bürgerkarte“ im Sinn des E-GovG somit nicht um eine physische, real existierende Karte (wie beispielsweise eine Bankomatkarte oder die e-Card), sondern um ein Konzept zur Sicherstellung der eindeutigen Identität (§ 2 Z 2 E-GovG) des Urhebers und der Authentizität (§ 2 Z 5 E-GovG) eines elektronisch gestellten Anbringens oder einer sonstigen Willenserklärung (§ 4 Abs 1 E-GovG). Somit kann jede beliebige technische Implementierung als „Bürgerkarte“ bezeichnet werden, welche die gesetzlichen Anforderungen des Bürgerkartenkonzepts erfüllt. Es muss dieser technischen Implementierung lediglich möglich sein, eine qualifizierte elektronische Signatur iSd SigG über bestimmte Daten zu erstellen und die „Personenbindung“, die einen speziellen Datensatz darstellt, zu speichern. In Frage kommen dafür beispielsweise Smartcards[109] oder SIM-Karten. Somit ist es möglich, die Personenbindung auf bereits im Einsatz befindlichen Bankomatkarten oder e-Cards aufzubringen und diese in der Folge auch als Bürgerkarte zu verwenden.

5.3 Die qualifizierte elektronische Signatur

Das erste der beiden Charakteristika der Bürgerkarte neben der Personenbindung ist das Erfordernis einer qualifizierten elektronischen Signatur iSd § 2 Z 3a SigG. Das bedeutet, dass das gesamte Konzept der Bürgerkarte auf den Regelungen des SigG aufbaut und dessen Regelungen in diesem Bereich somit ebenfalls von Relevanz sind. Eine qualifiziere Signatur ist eine

- fortgeschrittene elektronische Signatur, die auf einem
- qualifizierten Zertifikat (Z 9) beruht und von einer
- sicheren Signaturerstellungseinheit erstellt wurde (Z 5).

[109] Dies sind Chipkarten, die über eine Recheneinheit verfügen wie zB Bankomatkarten oder die e-Card.

5.3.1 Die fortgeschrittene elektronische Signatur

Die fortgeschrittene elektronische Signatur ist in § 2 Z 3 SigG geregelt und muss die folgenden rechtlichen Anforderungen erfüllen:

a) Die Signatur ist ausschließlich dem Signator zugeordnet.
b) Die Signatur ermöglicht die Identifizierung des Signators.
c) Die Signatur wurde mit Mitteln erstellt, die der Signator unter seiner alleinigen Kontrolle halten kann.
d) Die Signatur ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass jede nachträgliche Veränderung der Daten festgestellt werden kann.

„Ausschließlich dem Signator zugeordnet" (lit a) bedeutet, dass die Signaturerstellungsdaten[110] (in der Diktion der Technologie der digitalen Signatur der Private Schlüssel) zumindest innerhalb eines ZDA nur ein einziges Mal an einen Signator[111] vergeben werden dürfen und auch nur diesem bekannt sein bzw sich in dessen Verfügungsbereich befinden dürfen. Gelangen die Signaturerstellungsdaten einer unberechtigten dritten Person zur Kenntnis, kann die Signatur nicht mehr ausschließlich der berechtigten Person zugeordnet werden, wodurch sie ihre Eigenschaft als fortgeschrittene elektronische Signatur verliert. Diese Bedingung gewährleistet somit die Authentizität eines signierten Dokuments[112], da durch die ausschließliche Zuordnung der Signatur zum Signator auch sichergestellt werden kann, dass das signierte Dokument tatsächlich von diesem stammt. Litera b fordert, dass aus der Signatur eindeutig die Identität des Signators hervorgehen muss. Dies bedeutet, dass sich mit einer Signaturprüfung Angaben bzw Informationen ableiten lassen müssen, welche Rückschluss auf die (eindeutige) Nämlichkeit des Signators geben. Dies wird dadurch gewährleistet, dass die Signaturerstellungsdaten nur dem Signator bekannt sein dürfen und die Signaturprüfdaten[113] (in der Diktion der Technologie der digitalen

---

[110] § 2 Z 4 SigG.
[111] § 2 Z 2 SigG. Dabei kann es sich um eine natürliche als auch juristische Person sowie sonstige rechtsfähige Einrichtungen handeln.
[112] AA *Brenn*, Signaturgesetz, 54: Der Autor ordnet die Funktionalität der Authentizitätsprüfung lit b zu, welche jedoch nur fordert, dass aus der Signatur der Signator zuverlässig identifiziert werden können muss, also die eindeutige Identität bzw Nämlichkeit des Signators festgestellt werden können muss. Der Zusammenhang zwischen Identität und Urheberschaft (Authentizität) wird jedoch bereits in lit a gefordert. Angemerkt sei jedoch, dass es sich bei dieser Diskussion um eine theoretische ohne praktische Auswirkungen handelt, da ohnedies sämtliche Literae erfüllt sein müssen, damit einer Signatur die Eigenschaft einer fortgeschrittenen zukommt.
[113] § 2 Z 6 SigG.

Signatur der Öffentliche Schlüssel) in einer für den Empfänger vertrauenswürdigen Weise mit den Identifikationsmerkmalen des Absenders verknüpft sind. Ist eine Signaturprüfung erfolgreich, so kann der Empfänger davon ausgehen, dass nur der entsprechende Absender, der die Verschlüsselung mit dem ausschließlich ihm bekannten Privaten Schlüssel vornahm, die Signatur erstellen konnte. Die Erstellung einer Signatur darf gem lit c nur mit solchen Mitteln möglich sein, die der Signator unter seiner alleinigen Kontrolle hat. Dafür ist erforderlich, dass ausschließlich ihm die Signaturerstellungsdaten bekannt sind und der Vorgang der Signaturerstellung nur dann ausgelöst werden kann, wenn dies bewusst durch den Signator erfolgt. Daher muss das Verfahren, welches diese Forderung technologisch umsetzt, derart konzipiert sein, dass die Funktionalität des Signaturerstellungsvorgangs nur von berechtigten Personen ausgelöst werden kann. Dies kann durch das Erfordernis einer PIN-Eingabe umgesetzt werden oder durch entsprechende Zugangsberechtigungen in einem ELAK-System, welches die Funktionalität der Signaturaufbringung den Benutzern gegenüber kapselt. In lit d wird normiert, dass mittels einer fortgeschrittenen elektronischen Signatur auch die Integrität der signierten Daten sichergestellt bzw geprüft werden können muss. Die Erfüllung dieser Forderung ist dem technischen Verfahren der digitalen Signatur ohnedies immanent.

5.3.2 Qualifizierte Zertifikate

Eine qualifizierte elektronische Signatur muss weiters auf einem qualifizierten Zertifikat (§ 2 Z 9 SigG) beruhen. Ein Zertifikat an sich ist „*eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird*“[114]. Aus einem Zertifikat ergibt sich somit die Bindung eines bestimmten Öffentlichen Schlüssels an die Identität einer natürlichen oder juristischen Person. Wird einem Empfänger somit zusätzlich zu einer digitalen Signatur auch ein Zertifikat übermittelt, kann er daraus sowohl die Identität des Absenders als auch die ihm zugeordneten Signaturprüfdaten auslesen. Verläuft eine Signaturprüfung unter Verwendung des in einem solchen Zertifikat erhaltenen Öffentlichen Schlüssels positiv, kann der Absender sicher sein, dass das Dokument auch von jener Person stammt, welche im Zertifikat aufscheint.

[114] § 2 Z 8 SigG.

Ein Problem ist jedoch, dass ein solches Zertifikat auch beliebig gefälscht werden kann. So ist es leicht möglich, sich selbst ein Schlüsselpaar zu erzeugen und aus dem Öffentlichen Schlüssel und beliebigen (falschen) Identifikationsmerkmalen ein Zertifikat zu erzeugen. Daher muss das Zertifikat dem Empfänger entweder vor der ersten Kommunikation auf einem vertraulichen Weg übermittelt werden oder von einer vertrauenswürdigen dritten Stelle (digital) bestätigt werden, dass die Zuordnung des Öffentlichen Schlüssels zu den Identifikationsmerkmalen des Signators korrekt und authentisch ist. Solche vertrauenswürdigen dritten Parteien sind bei elektronischen Signaturen die Zertifizierungsdiensteanbieter (ZDA), die das Zertifikat für ein bestehendes vom Signator generiertes Schlüsselpaar zertifizieren[115]. Somit ist es erforderlich, dass ein qualifiziertes Zertifikat von einem ZDA iSd § 7 SigG zertifiziert sein muss. Dies geschieht dadurch, dass sich der ZDA von der Identität des Zertifikatswerbers entsprechend überzeugt und im Anschluss das elektronische Zertifikat seinerseits digital signiert.

Als drittes Erfordernis, damit ein Zertifikat als qualifiziertes Zertifikat anzusehen ist, muss das Zertifikat zumindest die Angaben des § 5 SigG beinhalten, wobei darüber hinaus auch weitere Angaben aufgenommen werden können.[116] Das Zertifikat mit allen beinhalteten Angaben muss – wie bereits erörtert – mit der fortgeschrittenen elektronischen Signatur des ZDA versehen werden (§ 5 Abs 3 SigG).

5.3.3 Sichere Signaturerstellungseinheiten

Bei einer sicheren Signaturerstellungseinheit handelt es sich um „*eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird und die den Sicherheitsanforderungen dieses Bundesgesetzes sowie der auf seiner Grundlage erlassenen Verordnungen entspricht*“.[117] Es müssen daher die in § 18 SigG und der Signaturverordnung aufgestellten technischen Sicherheitserfordernisse erfüllt werden.

---

[115] Eine solche Zertifizierung erfolgt selbst mittels einer Digitalen Signatur des Zertifikats mit dem Privaten Schlüssel des ZDA. Auf diese Weise kann eine beliebig lange Zertifikatskette („Chain of Trust“) erzeugt werden, wobei das „oberste“ Zertifikat („Wurzelzertifikat“) auf diese Weise nicht mehr weiter geprüft werden kann. Das Vertrauen in den öffentlichen Schlüssel dieses letzten ZDA muss auf andere Art und Weise sichergestellt werden (zB Abruf in vertrauenswürdigen Zertifikatsverzeichnissen, SSL-gesichert über die Homepage des ZDA, etc).

[116] Welche Angaben § 5 SigG genau fordert, kann dem Gesetz entnommen werden.

[117] § 2 Z 5 SigG.

5.3.4 Digitale Repräsentation von Zertifikaten

Wurde ein Zertifikat von einem ZDA digital signiert, so ist es für eine sichere Kommunikation nicht notwendig, dass die beiden kommunizierenden Parteien einander kennen. In einem solchen Fall reicht es aus, die Signatur des ZDA über das Zertifikat zu prüfen und die entsprechenden Informationen aus dem Zertifikat auszulesen. War die Signaturprüfung über das Zertifikat erfolgreich, kann auf die Richtigkeit der Angaben vertraut werden.

Damit sich aus den einzelnen Angaben in solchen Zertifikaten auch für Computersysteme die richtige Bedeutung (Semantik) erschließt, muss die Struktur des Zertifikats bekannt bzw standardisiert sein; es muss der Empfänger (bzw dessen Software zur Signaturprüfung) „wissen“, an welcher Stelle im Zertifikat sich welche Informationen befinden. Aus diesem Grund war es notwendig Standards einzuführen, wie solche Zertifikate digital zu strukturieren sind.

Der am weitesten verbreitete Standard für Softwarezertifikate ist X.509 (aktuell in der Version 3)[118]. Er definiert genau, welche Elemente das Zertifikat beinhalten muss, die vorgeschriebene Syntax, die standardisierte Bezeichnung für einen bestimmten Wert und den zulässigen Wertebereich. Neben den standardisierten Werten können in ein Zertifikat durch so genannte „Zertifikatserweiterungen“ auch beliebig weitere Werte eingefügt werden, die für eine Kommunikation zwischen zwei Parteien notwendig sind. Dies ergibt sich daraus, dass ein Zertifikat nicht für alle möglichen Anwendungsbereiche passend standardisiert werden kann. Folglich wird nur eine beschränkte Anzahl von Elementen standardmäßig aufgenommen, welche für eine Vielzahl von Kommunikationen notwendig sind. Durch Zertifikatserweiterungen können aber beliebig weitere Informationen für bestimmte Zwecke aufgenommen werden. Eine Zertifikatserweiterung besteht aus folgenden Elementen: eindeutige Kennzahl für die Erweiterung („Object Identifier“), ob die Angabe kritisch oder unkritisch ist und dem entsprechenden Wert.[119]

Eine Datei, die ein X.509-Zertifikat beinhaltet, ist in der Regel mit einer der folgenden Dateiendungen versehen: *.CER, *.CRT, *.DER, *.PEM, *.CSR, *.P12, *.P7B oder *.P7C.

[118] RFC 5280.
[119] Vgl RFC 5280.

5.4 Die Personenbindung

Kernelement zur eindeutigen Identifikation einer Person ist die auf der Bürgerkarte eingetragene Personenbindung. Die Personenbindung ist ein Datensatz, der in der Bürgerkarte dauerhaft gespeichert wird und zumindest folgende Elemente beinhaltet:

- Nachname und Vorname(n) bzw Bezeichnung der Person
- Geburtsdatum bei natürlichen Personen
- Stammzahl der Person, welche diese Österreich weit eindeutig identifiziert[120]
- Mindestens ein Zertifikat, welches den Öffentlichen Schlüssel der Person beinhaltet.

Dieser Datensatz wird vom Datenverarbeitungsregister als *Stammzahlenregisterbehörde* (§ 7 E-GovG) erstellt und im Zuge dieses einmaligen Erstellungsprozesses auf die Bürgerkarte aufgebracht. Er dient dem Nachweis der eindeutigen Identität des Einschreiters und der Authentizität des Anbringens. Der Datensatz der Personenbindung wird seinerseits von der Stammzahlenregisterbehörde digital signiert, wodurch die Authentizität der Personenbindung sichergestellt wird. Die Eintragung auf der Bürgerkarte erfolgt ebenfalls durch die Stammzahlenregisterbehörde oder durch andere Behörden oder sonstige geeignete Stellen in deren Auftrag.[121]

5.4.1 Verfahren zur Feststellung der Identität und Authentizität

Möchte sich nun ein Benutzer Zugang zu einer Behördenapplikation verschaffen, so wird dafür im ersten Schritt die Personenbindung zum Nachweis der eindeutigen Identität aus der Bürgerkarte ausgelesen, wofür die Eingabe einer PIN notwendig ist. Auf Grund der Stammzahl in dieser Personenbindung kann die Person nun eindeutig identifiziert werden (vgl § 4 Abs 2 E-GovG). Im zweiten Schritt wird der Bürgerkartenumgebung eine beliebige Zeichenkette[122] übergeben, welche nun nach Eingabe der Signatur-PIN[123] durch den Einschreiter von der Bürgerkartenumgebung digital signiert und an die Behördenapplikation zurückgegeben wird. Die Behördenapplikati-

[120] Auch für natürliche Personen wird hier die Stammzahl gespeichert, da das bPK erst bei Bedarf draus abgeleitet wird.
[121] § 4 Abs 2 E-GovG.
[122] In der Regel werden die aus der Personenbindung ausgelesenen Daten zur Person des Einschreiters in diese Zeichenkette mit einbezogen. Das sind idR Vor- und Nachname sowie Geburtsdatum.
[123] Dabei handelt es sich um eine andere PIN als jene, welche für das Auslesen der Personenbindung notwendig ist.

on muss nun die Gültigkeit des Zertifikats des Einschreiters, welches aus der Personenbindung ausgelesen wurde, auf Gültigkeit prüfen und den Öffentlichen Schlüssel extrahieren. Im Zuge der Zertifikatsprüfung ist festzustellen, dass das Zertifikat noch nicht abgelaufen ist, nicht widerrufen wurde und von einem zugelassenen ZDA zertifiziert wurde. Nach erfolgreicher Prüfung der vom Einschreiter digital signierten Zeichenkette gilt der Nachweis der Authentizität als erbracht (vgl § 4 Abs 4 E-GovG).

5.4.2 Die Stammzahl als Kernelement der Identifikation

Kernelement der eindeutigen Identifizierung ist die in der Personenbindung beinhaltete Stammzahl (§ 6 Abs 1 E-GovG). Die Stammzahl lässt sich nur einer einzigen Person zuordnen und ist daher Österreich weit ein eindeutiges Identifikationsmerkmal. Die Stammzahl ist die umkehrbare Ableitung aus einer bereits existierenden eindeutigen Kennnummer oder die direkte Verwendung dieser Kennummer. Daraus leitet sich auch die Bezeichnung „Personenbindung“ ab, da die Stammzahl und das qualifizierte Zertifikat somit einer eindeutigen Person zugeordnet werden können. Abhängig davon, welche Art von Person die Stammzahl identifizieren soll, kommen dafür unterschiedliche bereits existierende Kennungen in Frage:

Natürliche Personen: Die Stammzahl natürlicher Personen ergibt sich gem § 6 Abs 2 E-GovG aus einer Ableitung aus der ZMR-Zahl, die für jede in Österreich gemeldete natürliche Person mit Eintragung in das Zentrale Melderegister erstellt wird und diese eindeutig identifiziert. Aus Datenschutzgründen wird die Stammzahl bei natürlichen Personen jedoch nicht direkt verwendet, sondern umkehrbar aus der ZMR-Zahl errechnet. Diese Ableitung erfolgt durch symmetrische Verschlüsselung (Triple-DES[124]) der ZMR-Zahl mit einem ausschließlich der Stammzahlenregisterbehörde bekannten Verschlüsselungsschlüssel. Nur dieser Behörde ist es somit möglich, die Stammzahl auf die ZMR-Zahl zurückzuführen. Das Verfahren zur Verschlüsselung ist im Internet zu veröffentlichen (§ 6 Abs 6 E-GovG).

Beim Stammzahlenregister für natürliche Personen handelt es sich um ein so genanntes *„virtuelles Register“*, was bedeutet, dass Stammzahlen von der Stammzahlenregisterbehörde nicht dauerhaft (zB in einer Datenbank) gespeichert werden dürfen, sondern ausschließlich nur im Bedarfsfall aus der ZMR-Zahl abgeleitet werden

[124] *Hollosi/Hörbe*, Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK), 3.

dürfen. Somit muss die Stammzahlenregisterbehörde jedes Mal aufs Neue die Stammzahl aus der ZMR-Zahl berechnen, wenn diese (zulässiger Weise) benötigt wird (§ 12 Abs 1 Z 2 E-GovG). Unmittelbar im Anschluss ist diese wieder zu löschen.[125] Eine dauerhafte Speicherung der Stammzahl darf ausschließlich in der Bürgerkarte des Betroffenen erfolgen und auch dort nur in Form der Personenbindung (§ 12 Abs 1 Z 1 E-GovG). Unter „dauernd" wird wohl die Speicherung auf einem zur persistenten Datenspeicherung geeigneten Datenträger wie zB Smartcard, Festplatte, Datenbank, USB-Sticks etc zu verstehen sein, eine vorübergehende Speicherung in einem flüchtigen Datenspeicher wie RAM oder Cache wird im Zuge des Errechungsvorgangs des bPK jedoch zulässig und auch notwendig sein (§ 12 Abs 1 Z 3 E-GovG).

Juristische Personen: Bei juristischen Personen, die bereits in irgendein Register in Österreich eingetragen sind, wird die in diesem Register verwendete Kennnummer direkt und ohne Ableitung oder Verschlüsselung als Stammzahl verwendet. Aktuell sind dies beispielsweise die Firmenbuchnummer oder die Vereinsnummer aus dem ZVR. Da diese Kennnummern ohnedies öffentlich sind und unter bestimmten Umständen auch öffentlich angeführt werden müssen (vgl § 14 UGB), ist deren Verschlüsselung aus datenschutzrechtlichen Gesichtspunkten nicht notwendig. Die Stammzahl juristischer Personen unterliegt auch keinem besonderen Schutz (§ 12 Abs 1 E-GovG).

Nicht in Registern geführte Personen: Für Personen, die in Österreich in keinem Register geführt werden, wurde das „Ergänzungsregister" geschaffen, in welches solche Personen bei Ausstellung der Bürgerkarte eingetragen werden (§ 6 Abs 4 E-GovG). Für natürliche Personen besteht dafür das *„Ergänzungsregister für natürliche Personen"* (ERnP)[126] und für juristische Personen das *„Ergänzungsregister für sonstige Betroffene"* (ERsB). Hier ergibt sich die Stammzahl aus der Kennnummer im Ergänzungsregister („Ordnungsnummer").

Verfahren zur Erzeugung der Stammzahl: Die ZMR-Zahl oder Ordnungsnummer natürlicher Personen (in der Folge „Basiszahl") ist eine 12stellige Dezimalzahl. Zur

[125] *Dohr/Pollirer/Weiss*, E-GovG, 23.

[126] Hier werden natürliche Personen eingetragen, die keinen Wohnsitz in Österreich haben und dennoch eine Bürgerkarte benötigen (zB Auslandsösterreicher).

Berechnung der Stammzahl wird diese Dezimalzahl in eine binäre Darstellung übergeführt und auf folgende Weise auf 128 Bit erweitert: `Basiszahl Seed Basiszahl Basiszahl`. Seed ist eine 8 Bit große Zahl, die nur der Stammzahlenregisterbehörde bekannt ist. Diese Zahl wird nun mit dem Triple-DES-Algorithmus im CBC-Verfahren mit dem nur der Stammzahlenregisterbehörde bekannten Verschlüsselungsschlüssel symmetrisch verschlüsselt. Dieser Wert wird anschließend zur erleichterten Darstellbarkeit base64-codert.[127]

5.5 Die Identifikation natürlicher Personen in Datenanwendungen

Die Stammzahl ist somit eine für ganz Österreich eindeutige Kennnummer, mit welcher eine Person eindeutig identifiziert werden kann. Etwaig bestehende Verwechslungsrisiken (wie beispielsweise Namens- und Adressidentität) können durch Verwendung dieser Stammzahl mit Sicherheit ausgeschlossen werden. Doch genau diese Eindeutigkeit birgt für die Betroffenen auch gewisse Risiken: Sämtliche zu einer Person bestehenden Daten könnten über diese Kennnummer ohne Fehlerwahrscheinlichkeit über alle Verwaltungsbereiche hinweg zusammengeführt werden, woraus sich die Befürchtung des dadurch entstehenden „Gläsernen Bürgers“ ergab. Aus diesem Grund darf gem § 8 E-GovG für natürliche Personen in Datenanwendungen von Auftraggebern des öffentlichen Bereichs niemals die Stammzahl selbst zur Identifikation des Bürgers gespeichert werden, sondern lediglich ein *„bereichspezifisches Personenkennzeichen“* kurz *bPK*. Für juristische Personen darf hingegen die Stammzahl selbst gespeichert werden, da diesbezüglich ohnedies aus Datenschutzsicht keine Bedenken bestehen. Das bereichsspezifische Personenkennzeichen wird gesondert für jeden Verwaltungsbereich in einem unumkehrbaren Verfahren – einem Hash-Verfahren – aus der Stammzahl abgeleitet (§ 13 Abs 1 E-GovG) und behält dadurch die identifizierende Funktion der Stammzahl bei (§ 9 Abs 1 E-GovG). Dadurch, dass in die Ableitung auch der jeweilige Verwaltungsbereich mit einbezogen wird, ist eine Identifikation des Betroffenen nur in diesem Verwaltungsbereich möglich, nicht aber in anderen. Dadurch ist ein Datenabgleich oder eine Datenzusammenführung über Verwaltungsbereiche hinweg technisch nicht durchführbar. Auch eine Rückführung des bPK in die Stammzahl ist nicht möglich.

[127] *Hollosi/Hörbe*, Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK), 3.

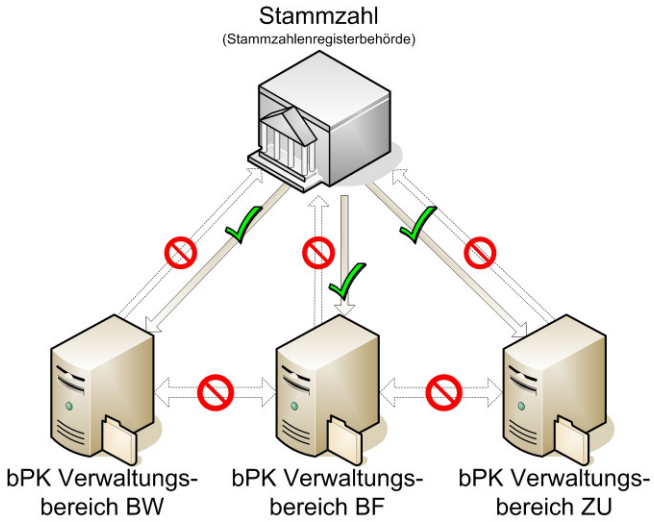

Abbildung 7: Mögliche Ableitungen

Diese Grafik stellt die möglichen Ableitungen nun übersichtlich dar: Aus der Stammzahl kann zwar das bPK des jeweiligen Verwaltungsbereichs (zB „BW“ für Bauen und Wohnen, “ZU“ für Zustellung, etc) berechnet werden, nicht jedoch die Stammzahl aus dem bPK. Auch eine „Umrechnung“ eines bPKs in jenes eines anderen Verwaltungsbereichs ist nicht möglich. Für die Ableitung des bPKs wird die Stammzahl in Base64-codierter Form als Zeichenkette mit einem + (als Zeichen), der fixen Zeichenkette `urn:publicid:gv.at:cdid+` und dem Kürzel des jeweiligen Verwaltungsbereichs – ebenfalls in der Form einer Zeichenkette – verbunden. Die einzelnen Verwaltungsbereiche und entsprechenden Kürzel sind in der E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV)[128] basierend auf § 9 Abs 2 E-GovG definiert, wobei das Kürzel in der Regel aus 2, maximal jedoch 5 Zeichen besteht. Aus dieser Zeichenkette wird nun mit dem SHA-1-Verfahren der Hashwert gebildet und gegebenenfalls in eine Base64-codierte Form übergeführt.[129] § 9 Abs 3 E-GovG sieht der Publizität halber vor, dass das für die Ableitung einzusetzende Verfahren im Internet zu veröffentlichen ist. Lediglich der verwendete Verschlüsselungsschlüssel ist (nahe liegender Weise) davon ausgenommen. Die Verfahren und Algorithmen werden im Dokument *Hollosi/Hörbe*, Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK) beschrieben und ist unter http://portal.bmi.gv.at/ref/portref/files/anleitungen/Stammzahl-bPK-Algorithmen.doc (Stand: 12. 6. 2011) verfügbar.

[128] Verordnung des Bundeskanzlers, mit der staatliche Tätigkeitsbereiche für Zwecke der Identifikation in E-Government-Kommunikationen abgegrenzt werden (BGBl II 289/2004).
[129] *Hollosi/Hörbe*, Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK), 4.

5.6 Verbot der Offenlegung von bPKs

Bereichspezifische Personenkennzeichen dienen ausschließlich der applikationsinternen Verwaltung und dürfen dem Betroffenen gegenüber nicht offen gelegt werden (§ 11 E-GovG). Um bestimmte Schriftstücke und Dokumente dennoch einem bestimmten Verfahren zuordnen zu können, muss ein anderes Verfahrenskennzeichen oder eine Geschäftszahl geführt werden, welche(s) gegebenenfalls dem Betroffenen gegenüber auf Schriftstücken anzuführen ist und auf welches er sich beziehen kann. Dadurch soll verhindert werden, dass durch Sammlung von Ausfertigungen zu einer Person aus verschiedensten Verwaltungsbereichen, auf welchen ansonsten ja das bPK in unverschlüsselter Form ausgewiesen wäre, bPKs auf eine Person rückgeführt werden können, wodurch das bPK-Konzept unterlaufen werden könnte. Es werden dadurch sektorspezifische Identifikatoren (zB SV-Nummer, Matrikelnummer, Passnummer) nicht verdrängt, sondern das bPK tritt zur internen Verarbeitung neben diese.[130]

5.7 Verfahren zur Erzeugung von bPK

Detaillierte Regelungen zu den Voraussetzungen, die für eine zulässige Erzeugung von bPKs erfüllt sein müssen, finden sich in § 10 E-GovG. Dies bedeutet, dass bPKs nicht von jedermann und nach Belieben erzeugt werden dürfen, sondern ausschließlich von ganz bestimmten Auftraggebern iSd DSG und dies auch nur unter bestimmten Voraussetzungen. Da es sich bei bPKs um personenbezogene Daten handelt, müssen darüber hinaus auch die Erfordernisse des DSG erfüllt sein, damit diese zulässiger Weise verarbeitet werden dürfen. § 3 Abs 2 E-GovG schränkt die Zulässigkeit der Verarbeitung von bPKs noch weiter ein, indem dieser regelt, dass die Identität eines mit einem Auftraggeber kommunizierenden Betroffenen nur dann erhoben bzw festgestellt und folglich gespeichert werden darf, wenn dies auf Grund eines berechtigten Interesses des Aufraggebers (zB zur Wahrung der ihm gesetzlich übertragenen Aufgaben) notwendig ist.

Prinzipiell dürfen bPKs sowohl von Auftraggebern des öffentlichen als auch des privaten Bereichs nur unter Mitwirkung des Betroffenen durch Einsatz seiner Bürgerkarte erzeugt werden, wobei der Betroffene über das Auslösen dieser Funktion infor-

[130] Vgl *Karning/Kustor*, E-Government in *Bauer/Reimer*, Handbuch Datenschutzrecht, 241.

miert sein muss (§ 12 Abs 2 Z 1 E-GovG). Dies kann beispielsweise durch das Erfordernis einer PIN-Eingabe[131] oder der Eingabe einer Telefonnummer einschließlich Passwort wie bei der Mobilen Signatur[132] erfüllt werden.

Ohne Mitwirkung des Betroffenen ist die Bildung eines bPKs nur der Stammzahlenregisterbehörde erlaubt. Wird ihr der entsprechende Verwaltungsbereich, für welchen der Auftraggeber zur Vollziehung berufen ist, mitgeteilt, so kann sie aus der Stammzahl das bPK auch ohne den Betroffenen und ohne dessen Bürgerkarte direkt ableiten (§ 12 Abs 2 Z 2 E-GovG). Dies kann beispielsweise für eine Erstausstattung einer Datenanwendung[133] eines Aufraggebers des öffentlichen Bereichs mit bPK notwendig sein, wenn für den Betroffenen bereits bei der erstmaligen Interaktion mit der Datenanwendung das bPK vorhanden sein muss. Für die elektronische Zustellung ist dies nicht notwendig, da es ausreichend ist, wenn das bPK bei der erstmaligen Anmeldung des Kunden erzeugt wird[134]. Eine solche Erstausstattung war beispielsweise bei der ÖH-Wahl 2009, die mittels E-Voting durchgeführt wurde, notwendig, da die bPKs der Wahlberechtigten zur eindeutigen Identifikation vor der Wahlhandlung bereits in der Datenanwendung vorhanden sein mussten.[135]

5.8 BPKs für fremde Verwaltungsbereiche

Trotz der strikten Trennung der einzelnen Verwaltungsbereiche durch die E-GovBerAbgrV können praktisch jedoch Fälle eintreten, in welchen es sehr wohl rechtlich zulässig und auch notwendig ist, dass die Daten eines Betroffenen aus mehreren Verwaltungsbereichen zusammengeführt werden müssen. Dies kann beispielsweise im Fall der Notwendigkeit von Amtshilfe oder einer sonstigen gesetzlich zulässigen Datenübermittlung[136] aus einem anderen Verwaltungsbereich notwendig werden. Ein weiteres in diesem Zusammenhang interessierendes Beispiel ist auch die elektronische Zustellung durch einen Zustelldienst: Für die Verfahrensabwicklung darf die

[131] Bei der Verwendung von Smartcards als Bürgerkarte kann beispielsweise die Personenbindung nur dann ausgelesen werden, wenn der Benutzer die korrekte PIN eingegeben hat.
[132] Vgl *Digitales Österreich*, Mobile Signature, http://www.buergerkarte.at/download/MobileSignatureSummary.pdf, abgerufen: 17. 1. 2012.
[133] Vgl Homepage der DSK, http://stammzahlenregister.gv.at/site/5975/default.aspx, abgerufen: 17. 1. 2012.
[134] Es wäre auch aus datenschutzrechtlicher Sicht keine Rechtfertigung zu erkennen, auf Grund welcher eine solche Speicherung zulässig wäre.
[135] Vgl BMWF, E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009 – Evaluierungsbericht, http://www.e-voting.cc/static/evoting/files/Evaluierungsbericht_E-Voting_Hochschuelerinnen-_und_Hochschuelerschaftswahlen_2009.pdf, abgerufen 17. 1. 2012.
[136] Vgl § 10 Abs 2 E-GovG.

Behörde das für ihren Zuständigkeitsbereich generierte bPK speichern, jedoch stellt die Zustellung einen eigenen Verwaltungsbereich dar.[137] Somit kommt für ein und denselben Bürger bei der Behörde im Zuge der Abwicklung des Verwaltungsverfahrens ein anderes bPK zum Einsatz als beim Zustelldienst für die Durchführung der Zustellung. Möchte nun die Behörde dem Zustelldienst eine Ausfertigung zur Durchführung der Zustellung übergeben, so muss dieser auch das bPK des Verwaltungsbereichs der Zustellung bekannt sein und dieses dem Zustelldienst zusammen mit dem zuzustellenden Dokument übergeben werden. Würde dem Zustelldienst theoretisch das bPK des Verwaltungsbereichs der Behörde übergeben werden, könnte das Dokument nicht dem entsprechenden Empfänger zugeordnet werden, da bei einer Abholung durch diesen das bPK für den Bereich Zustellung (ZU) berechnet wird und somit diese beiden bPKs einander nicht entsprechen würden. Das bPK eines anderen Verwaltungsbereichs wird als „Fremd-bPK“ oder „fbPK“ bezeichnet.

5.8.1 Die Umrechung von bPKs

Wie in Kapitel 5.5 bereits dargestellt, ist es eine wesentliche Eigenschaft von bPKs, dass eine Rückrechnung auf die Stammzahl oder die „Umrechnung“ von bPKs des einen Bereichs auf jene eines anderen Bereichs (technisch) nicht möglich ist. Sollen jedoch bestimmte Daten eines Betroffenen einem anderen Verwaltungsbereich (zB der Zustellung) zur Verfügung gestellt werden, muss vom ursprünglichen Auftraggeber das bPK des „Zielbereichs“ mit übergeben werden, damit dort die Zuordnung zum entsprechenden Betroffenen korrekt erfolgen kann.

Die Aufgabe dieser „Umrechnung“ bzw „Transformation“ übernimmt die Stammzahlenregisterbehörde gemäß § 6 StZRegBehV und darf gem § 13 Abs 2 E-GovG auch nur von dieser übernommen werden. Da es sich beim SZR um ein virtuelles Register handelt, wodurch eine Stammzahl immer nur bei Bedarf aus der ZMR-Zahl generiert und im Anschluss unmittelbar wieder gelöscht wird, kann und darf auch die Zuordnung Stammzahl und entsprechende bPKs nicht gespeichert werden. Auf Grund der technischen Ausprägung von bPKs ist jedoch auch dem SZR eine Rückführung in die Stammzahl oder die Umrechnung von bPKs des einen Bereichs in jene eines anderen Bereichs nicht möglich. Daher müssen dem SZR bei einer solchen bPK-Abfrage das vorhandene bPK einschließlich bestimmter anderer identifizierender An-

[137] Vgl. Anlage zur E-Gov-BerAbgrV.

gaben des Betroffenen und der gewünschte Verwaltungsbereich, für welchen das bPK berechnet werden soll, übergeben werden. § 6 Abs 1 StZRegBehV sieht die folgenden notwendigen Angaben vor:

- Name des Betroffenen und ggf Geburtsdatum (falls nicht vorhanden ein anderes Identifikationsmerkmal)
- bPK des Betroffenen und Verwaltungsbereich des Anfragenden („Quellbereich“)
- Bezeichnung und Verwaltungsbereich des Auftraggebers, für den das (verschlüsselte) bPK generiert werden soll („Zielbereich“)

Das Wort „oder“ in § 6 Abs 1 Z 2 StZRegBehV zwischen der Anforderung der Angabe eines weiteren Datums und dem bPK des Betroffenen verwirrt, ist jedoch in der Hinsicht zu verstehen, dass a) ein weiteres Datum zur Identifikation des Betroffenen nur dann anzugeben ist, wenn das Geburtsdatum nicht bekannt ist und b) das bPK des Betroffenen und der Verwaltungsbereich jedenfalls anzugeben sind.[138]

Für die Berechnung eines bPKs für einen anderen Verwaltungsbereich muss somit die natürliche Person im ZMR eindeutig identifiziert, deren Stammzahl berechnet und daraus das bPK für den gewünschten Verwaltungsbereich abgeleitet werden. Um sicherstellen zu können, dass auch tatsächlich die richtige Person identifiziert wurde, wird neben dem bPK für den „Zielbereich“ auch jenes für den „Quellbereich“ abgeleitet und mit dem verglichen, welches von der Behörde im Zuge der Abfrage übergeben wurde. Stimmen beide überein, wurde die korrekte Person identifiziert. Bei dieser Vorgehensweise spricht man vom „Trial-and-Error-Prinzip“.

Technisch wird für eine solche bPK-Transformation (und auch für weitere andere Abfragen) von der Stammzahlenregisterbehörde permanent ein Webservice zur Verfügung gestellt, über welches diese Abfrage durchgeführt werden kann. Der technische Betrieb dieser Webservices erfolgt auf Grund von § 7 Abs 2 E-GovG durch das BMI als Dienstleister und stellt im Wesentlichen eine „ZMR-Abfrage“ dar. Details über die

[138] *Ehrenmüller*, SZR 2.0 Anwendungsdokumentation, 11 f.

einzelnen Parameter solcher Abfragen finden sich im Dokument *SZR 2.0 Anwendungsdokumentation*[139].

5.8.2 Die Verschlüsselung von Fremd-bPKs

Aus Datenschutzgründen dürfen bPKs in unverschlüsselter Form nur in jenen Verwaltungsbereichen gespeichert werden, für welche der Auftraggeber (also die Behörde) auch zur Vollziehung berufen ist (§ 13 Abs 3 E-GovG). Möchte ein Auftraggeber auch bPKs anderer („fremder") Verwaltungsbereiche speichern, so darf dies ausschließlich in verschlüsselter Form erfolgen. Führt nun ein Auftraggeber des öffentlichen Bereichs eine bPK-Transformation beim SZR durch, so darf dem Auftraggeber das bPK des „Zielbereichs" bereits vom SZR nur in verschlüsselter Form zur Verfügung gestellt werden (§ 10 Abs 2 IS E-GovG). Die Pflicht zur Verschlüsselung obliegt (nahe liegender Weise) somit nicht dem Anfragenden. Eine Entschlüsselung ist in der Folge nur jenem Auftraggeber möglich, durch welchen die zu übermittelnden Daten auch zulässiger Weise verwendet werden dürfen (§ 13 Abs 2 Z 1 E-GovG). Weiters müssen in die zu verschlüsselnde Zeichenkette weitere dem Anfordernden nicht bekannte variable Angaben mit einbezogen werden (Z 2). Darunter sind beliebige Zeichen zu verstehen, die die zu verschlüsselnde Zeichenkette auf jene bestimmte Länge „auffüllen", die der notwendigen Blockgröße des (blockorientierten) Verschlüsselungsalgorithmus (RSAES-OAEP) entspricht. Konkret handelt es sich dabei ua um das aktuelle Datum. Der Empfänger „weiß" auf Grund der Spezifikation für die Erstellung von fbPKs, an welcher Stelle in der Zeichenkette sich diese variablen Informationen befinden und kann diese nach Entschlüsselung somit wieder entfernen. Durch Einbeziehung dieser variablen Informationen weist ein verschlüsseltes bPK folglich auch einen gänzlich anderen Aufbau auf als ein unverschlüsseltes bPK, wodurch bereits aus dem bPK selbst erkennbar ist, ob es sich dabei um ein unverschlüsseltes oder verschlüsseltes bPK handelt. Die konkrete Vorschrift zur Erstellung von verschlüsselten Fremd-bPKs findet sich in der Spezifikation zur Bildung der Stammzahl und von bPKs[140].

Die Verschlüsselung der so gebildeten Zeichenkette erfolgt mit dem öffentlichen Schlüssel des Empfängers (Auftraggeber des „Zielbereichs"), wodurch gewährleistet

[139] *Ehrenmüller*, SZR 2.0 Anwendungsdokumentation, http://portal.bmi.gv.at/ref/portref/files/anleitungen/szr-2.0-anwenderdokumentation.pdf, abgerufen am 17. 1. 2012.
[140] *Hollosi/Hörbe*, Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK), 8f.

werden kann, dass tatsächlich nur der gewünschte Empfänger das Fremd-bPK entschlüsseln kann. Die Zertifikate mit den Öffentlichen Schlüsseln der jeweiligen Ziel-Behörden können in einem zentralen Verzeichnis abgerufen werden.[141]

5.9 Sinn und Zweck des bPK-Konzepts

Mit der Einführung des bPK-Konzepts im E-Government-Gesetz wurde in Österreich das so genannte „sektorale Modell" umgesetzt. Dieses sieht vor, dass für jeden öffentlichen Verwaltungsbereich ein eigener Identifikator (bPK) zur eindeutigen Identifikation des jeweiligen Bürgers zum Einsatz kommt, der aus einer bereichsübergreifenden eindeutigen Kennnummer (Stammzahl) unumkehrbar abgeleitet wird. Auf diese Art und Weise kann auch technisch sichergestellt werden, dass durch dieses Konzept zwar in jedem Verwaltungsbereich eine eindeutige Identifikation des Betroffenen möglich ist, die Möglichkeit einer Zusammenführung von Daten aus mehreren oder allen Verwaltungsbereichen jedoch technisch verhindert wird. Dies ergibt sich daraus, dass eine Ableitung der Stammzahl in das bPK zwar einfach möglich ist, eine Rückrechnung in die Stammzahl oder Umrechnung in das bPK eines anderen Verwaltungsbereichs jedoch nicht erfolgen kann.[142]

5.10 Besonderheiten von bPKs für private Auftraggeber

Das E-GovG ermöglicht in den §§ 14 und 15, dass das bPK-Konzept auch von Auftraggebern des privaten Bereichs verwendet werden darf, um damit die Identifikation natürlicher Personen zu ermöglichen. Die frühere Bezeichnung als „wirtschaftsbereichsspezifisches Personenkennzeichen" (wbPK) wurde mit der E-GovG-Novelle 2007 zwar aufgegeben, soll an dieser Stelle der Einfachheit halber jedoch weiter verwendet werden. Diese Änderung wird damit begründet, dass die frühere Bezeichnung inkonsistent gewesen wäre[143], was jedoch nicht ganz nachvollziehbar ist: Dem wbPK liegen einerseits andere Ausgangsdaten zu Grunde und andererseits unterscheidet sich der Einsatzbereich gravierend. Die Bezeichnung wbPK wurde in der Praxis jedoch bis heute beibehalten[144], die bPK-Spezifikation verwendet diese nach wie vor und auch in § 16 Abs 1 MeldeG wird nach wie vor explizit das wbPK ange-

[141] *Hörbe*, Anforderungen an das Stammzahlen-Register (SZR-N), 12.
[142] Vgl *Karning/Kustor*, E-Government in *Bauer/Reimer*, Handbuch Datenschutzrecht, 233.
[143] Erl zur RV 290 BlgNR 23. GP, 5.
[144] Vgl Homepage der Stammzahlenregisterbehörde,
http://stammzahlenregister.gv.at/site/6001/default.aspx#wbpk, abgerufen am 17. 1. 2012.

führt. Dies führt zu einer erheblichen gesetzlichen Inkonsistenz, da für den Begriff des *wbPK* in § 16 MeldeG nun keine Legaldefinition mehr existiert. Aus diesem Gesichtspunkt wäre dessen Wiedereinführung wünschenswert.

5.10.1 Gemeinsamkeiten und Unterschiede zum bPK

Die Generierung von wbPKs erfolgt analog zur Generierung von bPKs, nur wird bei der Berechnung statt des Kürzels des jeweiligen Verwaltungsbereichs (E-GovBerAbgrV) die Stammzahl des Auftraggebers des privaten Bereichs verwendet. Die Berechnungsvorschrift ist somit dieselbe wie bei einem bPK, nur dass an die Stelle der Zeichenkette mit dem Verwaltungsbereich eben die Zeichenkette mit der Stammzahl des Auftraggebers tritt. Beispielsweise wird anstatt der Zeichenkette `urn:publicid:gv.at:cdid+BW` (für den Bereich Bauen und Wohnen, BW) für ein Unternehmen die Zeichenkette mit dessen Firmenbuchnummer `urn:publicid:gv.at:wbpk+FN+123456i` verwendet. Detaillierte Informationen zur Berechnungsvorschrift von wbPKs findet sich im Dokument *Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK)*[145].

Somit hat ein und derselbe Betroffene bei jedem privaten Auftraggeber ein anderes wbPK, wodurch eine Zusammenführung von Daten mehrerer Auftraggeber über diesen Identifikator nicht möglich ist. Auch eine wbPK-Transformation ist nicht möglich oder vorgesehen. Jeder Auftraggeber des privaten Bereichs darf nur jene wbPKs verarbeiten, welche mit seiner eigenen Stammzahl erzeugt wurden, wodurch eine Übermittlung von wbPKs an andere Auftraggeber unzulässig ist (§ 14 Abs 2 E-GovG).

5.10.2 Die rechtlichen Voraussetzungen für die Erzeugung eines wbPK

Auch das wbPK darf nur auf 2 Weisen abgeleitet werden: Entweder unter Einsatz der Bürgerkarte durch den Betroffenen oder ohne dessen Mitwirkung durch das SZR, wobei das Gesetz offenbar die erste Variante als die zu bevorzugende betrachtet. Die Erzeugung eines wbPK durch das SZR ohne Mitwirkung des Betroffenen ist nur unter ganz bestimmten Voraussetzungen zulässig (§ 15 Abs 1 E-GovG):

[145] *Hollosi/Hörbe*, Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK), S 6f.

- Der Auftraggeber *muss* auf Grund einer gesetzlichen Bestimmung die Identität seiner Kunden festhalten.
- Die Verwendung der Daten erfolgt entsprechend den Bestimmungen des DSG.

5.10.3 Der Schutz der Stammzahl bei der Erzeugung von wbPK

Eine weitere Sicherheitsmaßnahme zum Schutz der Stammzahl sieht § 15 Abs 2 E-GovG vor: Demnach darf die Stammzahl in keiner Phase der Berechnung des wbPK einem Auftraggeber des privaten Bereichs zur Verfügung gestellt werden. Das bedeutet, dass das wbPK nicht in der technischen Infrastruktur (zB auf einem Server) des Auftraggebers berechnet werden darf, sondern ausschließlich in der Bürgerkartenumgebung des Betroffenen, die entweder lokal auf dessen Endgerät installiert ist oder online von einem vertrauenswürdigen Diensteanbieter zur Verfügung gestellt wird (zB MOCCA Online BKU). Erkennt die Bürgerkartenumgebung auf Grund der im Zertifikat des Auftraggebers fehlenden Verwaltungseigenschaft, dass es sich um einen solchen des privaten Bereichs handelt, so darf die Stammzahl dem Auftraggeber nicht zur Errechnung des wbPK zur Verfügung gestellt werden, sondern muss dieses unmittelbar selbst berechnen und der Anwendung zur Verfügung stellen.

5.10.4 Prüfung des wbPK

Der Nachteil für den privaten Auftraggeber bei dieser Lösung ist, dass dieser von der BKU nur das fertig abgeleitete wbPK erhält, nicht jedoch die Personenbindung mit der Stammzahl, aus der er das bPK selbst ableiten kann. Dadurch erschwert sich die Prüfung, ob das von der BKU übergebene wbPK tatsächlich jener Person zuzuordnen ist, als die sie sich ausgibt. Es ist dem Auftraggeber ja nicht möglich, die von der SZRB digital signierte Personenbindung auszulesen und so die Daten zur Person selbst zu erhalten, sondern ihm wird lediglich das wbPK übergeben. Die Identität kann gem § 15 Abs 2 lS E-GovG somit nur dadurch überprüft werden, dass der Auftraggeber beim ZMR/ERnP (Vorsicht: nicht beim SZR!) eine Abfrage gem § 16 Abs 1 MeldeG durchführt. Das ZMR ist ja ein öffentliches Register, in welchem der Hauptwohnsitz jeder in Österreich wohnhaften natürlichen Person relativ einfach abgefragt werden kann, andere Personen können im ERnP abgefragt werden. Dafür ist lediglich Vor- und Nachname der abzufragenden Person sowie ein weiteres

Merkmal wie zB Geburtsdatum, Geburtsort, etc notwendig. Auch das wbPK gem § 14 E-GovG kann das dritte Merkmal bilden.

Erhält nun der Auftraggeber von der BKU einer Person das von dieser generierte wbPK, so muss zur Identifikation der Person und Verifikation des wbPK eine Abfrage beim ZMR/ERnP mit den Parametern Vorname, Nachname und wbPK durchgeführt werden. Ergibt die Anfrage einen Treffer, sind diese drei Parameter gültig, ergab die Abfrage keinen Treffer, so stimmt das wbPK nicht mit dem angegebenen Vor- und Nachnamen überein. Im Zuge einer solchen Abfrage muss der Auftraggeber auch seine eigene Stammzahl an das ZMR zur Prüfung der Richtigkeit des wbPK übermitteln. Das ZMR ruft die verfügbaren Personen anhand von Vor- und Nachname ab und lässt sich vom SZR technisch transparent jeweils das entsprechende wbPK erzeugen. Durch Vergleich mit dem vom Anfragenden übergebenen wbPK kann sichergestellt werden, dass das wbPK tatsächlich dieser Person zuzuordnen ist.

5.11 Zusammenfassung

Das Bürgerkartenkonzept ermöglicht eine qualitätsvolle elektronische Kommunikation zwischen Bürgern und Behörden, bei welcher die eindeutige Identität des Einschreiters und auch die Authentizität (einschließlich Integrität) des Anbringens verlässlich festgestellt werden kann. Dadurch wird den Nachteilen einer ungesicherten Kommunikation über das Internet begegnet und ein für behördliches Handeln notwendiges Qualitätsniveau für Kommunikationsvorgänge geschaffen.

Durch Einführung der (w)bPK wurde ein sektorales Identifikationsmanagement-system geschaffen, das auf der einen Seite eine eindeutige elektronische Identifikation einer natürlichen Person ermöglicht, auf der anderen Seite aber auch den dadurch entstehenden Gefahren für die Privatsphäre der Betroffenen begegnet. Die Existenz einer österreichweiten Bürgeridentifikationsnummer wird so vermieden, wodurch Datenzusammenführungen mit technischen und nicht „bloß“ mit rechtlichen Mitteln verhindert werden. Missbrauch von (w)bPKs soll darüber hinaus durch entsprechende Strafbestimmungen verhindert werden (§ 22 E-GovG).

Auch für den Bereich der Zustellung kommt das Konzept der Bürgerkarte zwingend zur Anwendung (§§ 35 Abs 3 und 33 ZustG), wodurch auch für diesen Verwaltungsbereich die erörterten Regelungen des E-GovG voll zur Anwendung

kommen. Einerseits muss bereits bei der Anmeldung (oder auch Abmeldung) bei einem Zustelldienst und der damit verbundenen Einwilligung in die elektronische Zustellung von Dokumenten die Identität des Anmeldenden und auch die Authentizität dieser Einwilligung sichergestellt werden. Andererseits muss bei einer Abholung eines bei einem Zustelldienst bereit liegenden Dokuments nachweislich sichergestellt werden, dass das Dokument tatsächlich jenem Empfänger ausgefolgt wird, welcher in der Zustellverfügung der Behörde benannt wurde.

6. Die Aktualisierung des Zustellkopfs

§ 29 Abs 1 Z 1 ZustG sieht im Wesentlichen vor, dass sämtliche Änderungen von Kundendaten vom Zustelldienst unmittelbar an den Zustellkopf zu melden sind (*Aktualisierungsleistung*), welcher die Daten aller Kunden aller Zustelldienste zentral verwaltet (*Zentrale Speicherleistung*, § 29 Abs 2 Z 1 ZustG). Diese Daten können von zustellenden Behörden somit zentral bei einem einzigen (technischen) Dienst im Zuge der Adressierbarkeitsabfrage ermittelt werden.

Die *Zentrale Speicherleistung* umfasst die zustellsystemweite zentralisierte Verwaltung aller bei sämtlichen zugelassenen Zustelldiensten angemeldeten Kunden und bildet dadurch einen zentralen Verzeichnisdienst im gesamten Zustellsystem. Die konkrete technische Definition, wie dieser Datenspeicher zu implementieren ist und welche Eigenschaften dieser aufweisen muss, wird im Spezifikationsdokument ZUSELDAP[146] geregelt. Einerseits sind im Zuge der Zentralen Speicherleistung die in § 33 Abs 1 ZustG angeführten Daten stets in ihrer aktuellsten Form zu speichern, andererseits sind für jeden Kunden auch von diesem bekannt gegebene Abwesenheitsnotizen zu verwalten. Damit diese Daten im Zustellkopf stets aktuell sind, ist jeder Zustelldienst gesetzlich dazu verpflichtet, die Daten eines neu angemeldeten Kunden, Änderungen solcher Daten durch den Kunden oder durch den Kunden dem Zustelldienst gegenüber bekannt gegebene Abwesenheitsnotizen unverzüglich dem Zustellkopf mitzuteilen (*Aktualisierungsleistung*, § 29 Abs 1 Z 1 ZustG). Das zentrale Verzeichnis des Zustellkopfs ist folglich eine Akkumulation sämtlicher Kundendaten aller zugelassenen Zustelldienste.[147]

[146] *Tauber/Reichstädter*, ZUSELDAP.
[147] *Tauber/Reichstädter*, ZUSELDAP, 4.

6.1 Intention der Zentralen Speicherleistung

Sinn und Zweck dieser zentralen Speicherung der Daten aller bei einem elektronischen Zustelldienst angemeldeten Kunden ist, dass jeder potentielle Versender auf diese Weise nur eine einzige Stelle – nämlich den Zustellkopf – vor Durchführung einer elektronischen Zustellung abfragen muss, ob der Empfänger bei (irgend)einem elektronischen Zustelldienst gemeldet ist und gegebenenfalls bei welchem. Dadurch entfällt die Notwendigkeit, eine solche Abfrage bei jedem einzelnen zugelassenen Zustelldienst durchführen zu müssen.[148] Auch Daten zur inhaltlichen Verschlüsselung und die zulässigen Dateiformate können unmittelbar vom Zustellkopf verwaltet werden, wodurch eine zweimalige Abfrage – nämlich die erste, um zu erfahren, bei welchem oder welchen Zustelldienst(en) der Empfänger gemeldet ist und die zweite direkt beim gewählten Zustelldienst hinsichtlich der Verschlüsselungsdaten und Dateiformate – unterbleiben kann.

Diese technische Lösung ermöglicht es, die für die Durchführung einer Zustellleistung notwendigen Abfragen bzw Kommunikationen zwischen den einzelnen Zustelldiensten und Versendern auf ein Minimum zu reduzieren und so die Performance des gesamten Systems insgesamt wesentlich zu steigern. Ein nicht zu unterschätzender Nachteil dieser Lösung ist jedoch die Existenz einer einzigen zentralen Komponente, welche für das Funktionieren des Gesamtsystems und somit dessen Verfügbarkeit unabdingbar ist. Es handelt sich dabei um einen „Single Point of Failure“, also um den Teil eines technischen Systems, dessen Ausfall notwendigerweise den Ausfall des Gesamtsystems nach sich zieht.

6.2 Die eingesetzten Technologien

Damit der Zustellkopf die Zentrale Speicherleistung implementieren kann, muss dieser über einen entsprechenden Datenspeicher verfügen. Weiters ist die Bereitstellung definierter Schnittstellen erforderlich, über welche Daten in den zentralen Datenspeicher eingespeichert und wieder ausgelesen werden können. Die einheitliche Definition und Offenlegung solcher Schnittstellen ist deshalb notwendig, damit es jedem zugelassenen Zustelldienst technisch möglich ist, die Aktualisierungsleistung zu erbringen und Änderungen in seinem Datenbestand dem Zustellkopf mitteilen zu können.

[148] Vgl *Larcher*, Zustellrecht, RZ 482, mwN.

Wie die Bezeichnung der Spezifikation ZUSELDAP bereits erkennen lässt, muss für die zentrale Datenspeicherung beim Zustellkopf ein LDAP-Server zum Einsatz kommen. Die Verwendung einer anderen technischen Lösungsvariante – wie beispielsweise eines herkömmlichen SQL-basierten Datenbankservers – ist somit nicht möglich. Dies ergibt sich aus dem Umstand, dass auch jeder Zustelldienst bei sich „lokal" einen solchen LDAP-Server in derselben Ausformung wie beim Zustellkopf betreiben muss, welcher die Verwaltung der Kundendaten übernimmt. Kommt es nun zu Änderungen von Daten im LDAP-Server eines Zustelldienstes durch Anmeldung, Änderungsmeldung oder Abmeldung von Kunden, so speichert dies der jeweils betroffene Zustelldienst im ersten Schritt in seinem eigenen LDAP-Server ab. Erst im zweiten Schritt übergibt er die „Differenzdaten" in Form einer LDIF-Datei[149] an den Zustellkopf. Die technischen Anforderungen an diese Schnittstelle werden in der Spezifikation ZUSEPUSH detailliert beschrieben.

6.2.1 Der Standard Lightweight Directory Access Protocol (LDAP)

Bei LDAP (Lightweight Directory Access Protocol)[150] handelt es sich um ein standardisiertes Kommunikationsprotokoll zur Abfrage von (zentralen) Verzeichnissen über das Internet (genau das TCP/IP-Protokoll). LDAP-basierte Verzeichnisdienste kommen in der Regel dort zum Einsatz, wo Benutzerdaten oder sonstige zu verwaltende Informationen zentral verarbeitet werden sollen und in der Regel signifikant mehr Datenabfragen als Dateneinspeicherungen erfolgen. Die Stärke liegt dabei in der optimierten Lese- und Suchfunktionalität. LDAP stellt somit die definierte Schnittstelle für die Abfrage von Daten aus solchen zentralen LDAP-Servern dar.[151]

6.2.2 Das LDAP-Modell im Bereich der elektronischen Zustellung

Innerhalb des LDAP-Servers werden die Daten baumartig abgelegt, um diese rasch und einfach in strukturierter Form suchen und abrufen zu können. Dadurch können in einfacher Art und Weise auch Organisationsstrukturen und somit Über- und Unterordnungsverhältnisse abgebildet werden. Des Weiteren ermöglicht es diese Struktur, von einer allgemeinen Information durch einfache Entscheidung („Abzweigung") immer tiefer in den Baum zu der immer detaillierteren Information vorzudringen.

---

[149] RFC 2849.
[150] RFC 4510.
[151] *Zörner*, LDAP für Java-Entwickler, 27 ff.

Die Baumstruktur (Directory Information Tree, DIT) im LDAP-Server des Zustellkopfs stellt sich wie folgt dar:

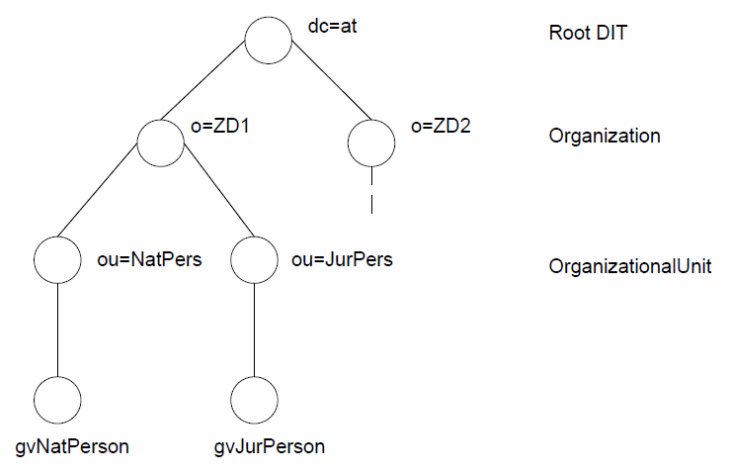

Abbildung 8: Die LDAP-Baumstruktur[152]

Das Wurzelelement (Root-Element) enthält stets die Domain Component (dc) „AT“ für Österreich. Dadurch wäre es theoretisch möglich, auch weitere Länder in das zentrale Kundenverzeichnis aufzunehmen, wodurch auch der europaweite bzw internationale Betrieb eines länderübergreifenden Zustellsystems möglich wäre. Die darunter liegende Ebene beinhaltet die Organisationen (o), die die einzelnen zugelassenen Zustelldienste repräsentieren. Erhält ein weiterer Zustelldienst eine Zulassung, so wird auf dieser Ebene ein weiteres Element mitsamt dem darunter liegenden Teilbaum erstellt. Dadurch erhält jeder Zustelldienst einen eigenen Namensraum. Ist ein und dieselbe Person bei mehreren Zustelldiensten angemeldet, so wird sie redundant in jedem Teilbaum des jeweiligen Zustelldienstes angelegt und wird technisch wie zwei voneinander verschiedene Personen behandelt. Dies ist auch notwendig, da beispielsweise bei mehreren Zustelldiensten unterschiedliche Verschlüsselungszertifikate hinterlegt werden können.

Auf Ebene der Organisationseinheit (ou) erfolgt eine Aufteilung in natürliche und juristische Personen, da je nach Art der Person unterschiedliche Daten zu speichern sind. Die einzelnen Elemente, welche die entsprechenden Daten zur Person beinhalten und je in beliebiger Anzahl vorkommen können, werden durch die Elemente „gvNat“ für natürliche Personen und „gvJur“ für juristische Personen dargestellt. Dies

[152] *Tauber/Reichstädter*, ZUSELDAP, 6.

ist die letzte Ebene im DIT, eine weitere hierarchische Untergliederung ist nicht mehr vorgesehen.[153]

Die Spezifikation ZUSELDAP beinhaltet in Kapitel 3 eine abschließende Aufzählung, welche Daten konkret vom Zustellkopf in welchem Datenformat zu speichern sind und gibt zum besseren Verständnis zu jedem Datum auch ein konkretes Beispiel. Weiters wird zu jedem Datum angegeben, ob dieses gespeichert werden muss (Mussfeld, gekennzeichnet mit „M“) oder fakultativ gespeichert werden kann (Kannfeld) und ob das Datenfeld pro Entität (also pro natürlicher oder juristischer Person) nur ein einziges Mal („single-valued“) vorkommen darf oder beliebig oft („multi-valued“, gekennzeichnet mit „L“). Beispielsweise hat eine natürliche Person lediglich einen Nachnamen, kann jedoch mehrere E-Mail-Adressen für Verständigungen haben. Dieser Datenkatalog umfasst im Wesentlichen die Daten des § 33 Abs 1 ZustG und Abwesenheitsnotizen.
Für natürliche Personen wird durch eine Abfrage im Zentralen Melderegister (ZMR) auch festgestellt, ob das Ergebnis der Abfrage eindeutig ist und somit die konkrete Person mit den vorliegenden Daten eindeutig[154] identifiziert werden kann. Diese Prüfung erfolgt bezüglich der Parameter Vorname-Nachname-Geburtsdatum obligatorisch und bezüglich Vorname-Nachname-Abgabestelle nur dann, wenn eine solche vom Kunden angegeben wurde. Das Ergebnis beider Prüfungen wird je mit dem Wert TRUE oder FALSE gespeichert.[155] Für juristische Personen ist darüber hinaus auch jenes Register anzugeben, in welchem sie geführt wird (ZVR, FB, ERsB).[156]

6.3 Die Aktualisierungsleistung

Als Teil der *Zustellleistung* hat jeder Zustelldienst die *„Aktualisierungsleistung“* gem § 29 Abs 1 Z 1 ZustG entsprechend dem Stand der Technik zu erbringen. Unter „Stand der Technik“ ist in diesem Zusammenhang gemäß der Spezifikation ZUSEPUSH zu verstehen. Darunter versteht das Gesetz die unverzügliche Weiterleitung folgender Daten an den Zustellkopf:

a) der Daten gemäß § 33 Abs 1

[153] *Tauber/Reichstädter*, ZUSELDAP, 6 f.
[154] § 2 Z 2 E-GovG.
[155] *Tauber*, ZUSEPUSH, 9.
[156] *Tauber/Reichstädter*, ZUSELDAP, 8.

b) einer vom Kunden bekannt gegebenen Änderung dieser Daten (§ 33 Abs 2 erster Satz)
c) von Mitteilungen gemäß § 33 Abs 2 zweiter Satz

Zusammengefasst umschreiben diese Leistungen jene Fälle, in welchen sich ein Kunde neu bei einem Zustelldienst angemeldet, seine Kundendaten ändert, sich abmeldet oder Abwesenheitsmitteilungen abgibt.

Wie eingangs beschrieben ist es nicht ausreichend, wenn der Zustelldienst solche Kundendaten und entsprechende Änderungen lediglich selbst in seinem LDAP-Server speichert, sondern er muss diese neuen oder geänderten Daten auch mit dem Datenbestand des Zustellkopfs abgleichen. Dafür ist es technisch notwendig, dass sowohl der Zustelldienst als auch der Zustellkopf über entsprechende Schnittstellen verfügen, über welche die beiden Computersysteme kommunizieren können, um diesen Datenabgleich durchzuführen.

Es handelt sich bei der *Aktualisierungsleistung* somit technisch um ein Replikationsverfahren: Grundsätzlich hält jeder Zustelldienst die Daten seiner Kunden in seinem eigenen LDAP-Server. Ergeben sich in diesem Datenbestand nun Änderungen, werden diese dem Zustellkopf mitgeteilt und dort ebenfalls aktualisiert („gepusht“). Dadurch stellt der Kundendatenbestand bei einem einzelnen Zustelldienst eine Teilmenge des Kundendatenbestandes des Zustellkopfs dar. Jeder Zustelldienst repliziert seinen Datenbestand in den LDAP-Server des Zustellkopfs und führt somit einen Datenabgleich durch. Dabei ist jedoch anzumerken, dass die Datenreplikation nur unidirektional, also vom Zustelldienst zum Zustellkopf und nicht umgekehrt erfolgt. Lediglich ein Statuswert wird zurückgegeben, welcher den Erfolg oder Misserfolg einer Transaktion bekannt gibt.

Anstoß des gesamten Vorgangs ist somit die Neuanmeldung eines Kunden, die Änderung von Kundendaten (einschließlich Abwesenheitsmitteilungen) durch einen bestehenden Kunden oder die Abmeldung eines Kunden. Jedes dieser Ereignisse löst gesetzlich verpflichtend *unverzüglich* die Ausführung der Aktualisierungsleistung aus. Im ersten Schritt werden die Kundendaten entsprechend im eigenen LDAP-Server des Zustelldienstes geändert. Im nächsten Schritt muss der Zustelldienst aus den

einzufügenden, zu ändernden oder zu löschenden Daten eine entsprechende LDIF-Datei erstellen, welche sowohl der Spezifikation LDAP Data Interchange Format (LDIF)[157] als auch ZUSEPUSH entspricht. Bei LDIF handelt es sich um ein standardisiertes Protokoll (Datenformat), welches dem Import oder Export von Informationen aus LDAP-basierten Verzeichnisservern oder zur Beschreibung einer oder mehrerer Änderungen in einem solchen Verzeichnis dient. Der Zustelldienst muss folglich nun einen spezifikationskonformen LDIF-Datensatz erstellen, welcher die gesamten dem Zustellkopf mitzuteilenden Informationen beinhaltet, und diese an den Zustellkopf übermitteln. In einem einzigen LDIF-Datensatz können ein oder auch mehrere Verzeichniseinträge geändert werden.

Der Ablauf der Aktualisierungsleistung lässt sich grafisch wie folgt darstellen:

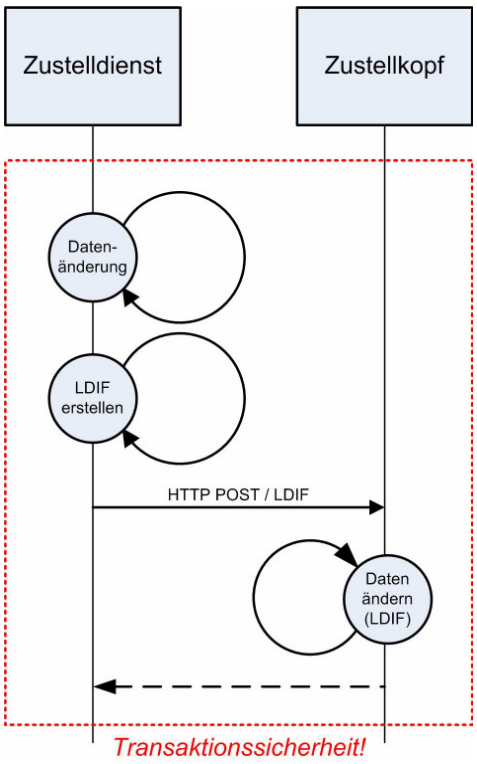

Abbildung 9: Der Ablauf der Aktualisierungsleistung[158]

Die Identifikation jenes Verzeichniseintrages, auf welchen sich eine LDIF-Änderungsanweisung bezieht, erfolgt durch den so genannten *Distinguished Name* (DN). Dieser besteht aus dem bPK (nP) bzw der Stammzahl (jP) jener Person, deren Daten geändert werden sollen und dienen somit der eindeutigen Identifikation jenes

[157] RFC 2849.
[158] *Tauber*, ZUSEPUSH, 5.

Teilbaumes, in welchem die Änderung durchgeführt werden soll. Ein Teilbaum wird durch Angabe der *Domain Component* (als Wurzelelement [derzeit noch] stets mit dem Wert „at"), der *Organization* („bz") und der *Organization Unit* (gvNatPers für eine natürliche Person) eindeutig identifiziert und spiegelt somit die in ZUSELDAP definierte Baumstruktur wider (vgl Abbildung 8). Das Attribut *changetype [add|modify|delete]* gibt an, welche Operation bezogen auf den gesamten Verzeichniseintrag durchzuführen ist und je nach durchzuführender Aktion sind entsprechend der LDIF-Spezifikation noch weitere Parameter anzugeben. Mit *changetype: modify* können auch einzelne Attribute eines Verzeichniseintrags hinzugefügt, modifiziert oder gelöscht werden.

Beispiel (ein angemeldeter Kunde hat seine Straße gelöscht):

```
dn:gvZbPK=iEaen9dEi6axEnxekyq93TsDlw9\=,ou=gvNatPers,o=bz,dc=at
changetype: modify
delete: street
```

Die Übermittlung erfolgt mittels eines HTTP-POST-Requests rein textbasiert über eine verschlüsselte Internetverbindung. Die Verschlüsselung dieser Verbindung muss entsprechend ZUSEPUSH verpflichtend mit dem Protokoll TLS (Transport Layer Security)[159] erfolgen. Die Bezeichnung *TLS* ist bis dato noch wenig verbreitet, beschreibt jedoch lediglich eine Nachfolgerversion des weitläufig bekannten SSL-Protokolls.[160] Damit der Server des Zustellkopfs den Aufbau einer solchen SSL-Verbindung zulässt, muss erstmalig das Zertifikat des Zustelldienstes in diesem hinterlegt werden. Auf diese Weise kann Missbrauch begegnet werden, da der Zustellkopf den SSL-Verbindungsaufbau verweigert, wenn ihm das Clientzertifikat, mit welchem die Verbindung aufgebaut werden soll, nicht bekannt ist.

Im letzten Schritt verarbeitet nun der Zustellkopf die ihm übermittelte LDIF-Datei, indem er die Anweisungen in seinen LDAP-Server übernimmt. Dabei ist darauf zu achten, dass nur solche Anweisungen ausgeführt werden dürfen, welche sich auch auf den entsprechenden Teilbaum des Zustelldienstes beziehen. Es darf einem Zustelldienst somit nicht möglich sein, im Zustellkopf Kundendaten eines anderen Zustelldienstes (also in dessen Teilbaum) zu manipulieren. Beziehen sich einzelne Ände-

[159] RFC 5246, 2818.
[160] Version 1.0 des TLS-Protokolls entspricht der Version 3.1 von SSL.

rungsdaten auf Verzeichnisdaten natürlicher Personen, so sind die Parameter Vorname-Nachname-Geburtsdatum sowie Vorname-Nachname-Abgabestelle auf deren Eindeutigkeit mit dem ZMR abzugleichen. Liegt Eindeutigkeit vor, so ist diese Information im LDAP-Verzeichnis zu vermerken.[161]

Abschließend übermittelt der Zustellkopf jenem Zustelldienst, der die Änderungsanfrage gestellt hat, eine entsprechende Erfolgs- oder Fehlermeldung. Dies erfolgt in Form einer XML-Datei, welche direkt in den HTTP-Body der *PushResponse* als Antwort auf den HTTP-POST-Request eingebettet wird. Die Struktur dieser XML-Antwort ist in der XML-Schema-Datei *zkopf.xsd* (am Ende) definiert, welche der gesamten Zustellungsspezifikation als normativer Bestandteil beiliegt. Sie enthält bestenfalls nur ein Element, nämlich das *Success*-Element im Erfolgsfall. Anderenfalls wird ein *Error*-Element[162] eingebettet, wenn ein allgemeiner Fehler auftrat, oder mehrere *Error*-Elemente, wenn bei der Übernahme einzelner Änderungsanforderungen ein Fehler auftrat[163]. Diese XML-Datenstruktur wird abschließend an den Zustelldienst über die verschlüsselte TLS-Verbindung rückübermittelt, womit die *Aktualisierungsleistung* abgeschlossen ist.

Beispiel einer Erfolgsmeldung im XML-Format:

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=UTF-8
Content-Length: 11111

<?xml version="1.0" encoding="UTF-8"?>
<PushResponse xmlns="http://reference.e-
government.gv.at/namespace/zustellung/kopf">
      <Success/>
</PushResponse>
```

Für die gesamte Aktualisierungsleistung ist ein Transaktionsmechanismus zu implementieren. Dies bedeutet, dass technisch sichergestellt werden muss, dass die Datenbestände des Zustelldienstes und des Zustellkopfes konsistent bleiben. Tritt irgendwo bei der Aktualisierung des Zustellkopfs ein Fehler auf, ist dies in der Antwort

[161] Dafür sieht ZUSELDAP die beiden LDAP Attribute *gvCRRBirthDate* und *gvCRRAddress* vor.

[162] Die XML-Struktur beinhaltet in diesem Fall als Rückgabewert einen Fehlercode und eine textliche Beschreibung des Fehlers.

[163] Die XML-Struktur beinhaltet in diesem Fall als Rückgabewert pro fehlgeschlagenem Verzeichniselement den *Distinguished Name* (DN) als eindeutige Identifikation des zu ändernden Objekts und eine allgemeine textliche Beschreibung.

an den Zustelldienst als entsprechendes Error-Element anzuführen. Kann die Erfolgs- bzw Fehlermeldung nicht an den Zustelldienst übermittelt werden (zB dieser ist aktuell nicht verfügbar) müssen alle bereits durchgeführten Änderungen im Zustellkopf rückgängig gemacht werden. Der Zustelldienst muss seinerseits so lange den LDIF-Datensatz an den Zustellkopf übermitteln, bis er eine Erfolgsmeldung erhält.[164]

7. Die Ermittlungsleistung

Die Ermittlungsleistung eröffnet einer Behörde, die eine Zustellung eines Dokuments an einen bestimmten Empfänger verfügen möchte, die Möglichkeit zu ermitteln, ob dieser Empfänger überhaupt bei (irgend)einem elektronischen Zustelldienst angemeldet ist und gegebenenfalls bei welchem. Diese Leistung basiert folglich auf der *Zentralen Speicherleistung* und der *Aktualisierungsleistung*, denn nur wenn die Daten beim Zustellkopf als zentralen Verzeichnisdienst verfügbar und akkurat sind, liefert eine solche Abfrage korrekte Ergebnisse. Als Antwort auf die Anfrage einer Behörde übermittelt der Zustelldienst einen Antwortdatensatz, der die entsprechenden Informationen für die weitere Durchführung des Zustellvorgangs beinhaltet (§ 34 Abs 1 ZustG).

Damit technisch die Möglichkeit geschaffen werden kann, einer Vielzahl von Behörden die Abfrage beim Zustellkopf zu ermöglichen, bedarf es analog zur *Aktualisierungsleistung* der Definition und Implementierung offener und standardisierter Schnittstellen. Ist die Definition einer Schnittstelle hinlänglich offen gelegt, besteht die Möglichkeit, solche Schnittstellen anzusprechen und die „dahinter liegende“ Funktionalität des Systems zu verwenden, ohne deren konkrete Implementierung zu kennen. Die Schnittstelle zwischen dem Zustellkopf und einer zustellenden Behörde für eine Abfrage ist in der Spezifikation ZUSEKOPF und technisch in der Datei *zkopf.xsd* definiert. Sie konkretisiert, welche Daten dem Zustellkopf im Zuge einer Abfrage übermittelt und wie diese strukturiert werden müssen. Korrespondierend wird auch genau festgelegt, welche Daten der Zustellkopf als Antwort liefert und wie diese strukturiert sind. Darüber hinaus beinhaltet die Spezifikation noch einige allgemeine Anforderungen, die erfüllt sein müssen, um eine sichere Kommunikation zwischen Zustellkopf und Absender zu gewährleisten.

[164] Vgl *Tauber*, ZUSEPUSH, 5.

Die gesetzlichen Regelungen für die Inanspruchnahme der Ermittlungsleistung finden sich in § 34 ZustG und beinhalten detaillierte Regelungen, unter welchen Voraussetzungen eine Abfrage des Zustellkopfs gesetzlich zulässig ist, welche Suchparameter verwendet werden dürfen und welche Daten dem Absender vom Zustellkopf in der Antwort zu übermitteln[165] sind. Die Antwort des Zustellkopfs liefert der Behörde die Information, ob eine elektronische Zustellung überhaupt möglich ist, also der Empfänger bei einem Zustelldienst angemeldet ist, und (kumulativ) ob die Zustellung für den aktuellen Zeitpunkt nicht gem § 33 Abs 2 ZustG ausgeschlossen wurde (§ 34 Abs 1 Z 2 ZustG). Weiters beinhaltet der Antwortdatensatz im Erfolgsfall die entsprechenden Informationen zur Auswahl des zu beauftragenden Zustelldienstes.

7.1 Zulässige Suchkriterien

Um zu verhindern, dass der Zustellkopf missbräuchlich verwendet wird oder diesem unrechtmäßig Daten „entlockt" werden, schränkt das Zustellgesetz die für die Durchführung einer Adressierbarkeitsabfrage zulässigen Parameter ein. § 34 Abs 2 IS ZustG sieht vor, dass für eine solche Abfrage ausschließlich (taxativ) die in § 33 Abs 1 Z 1 – 5 ZustG aufgelisteten Parameter verwendet werden dürfen:

- Name bzw. Bezeichnung des Kunden
- Geburtsdatum (bei natürlichen Personen)
- bPK bzw SZ
- die elektronische Verständigungsadresse
- die physische Verständigungsadresse

Eine nähere Regelung, ob für eine Abfrage nur jeweils ein einzelner Parameter verwendet werden darf oder in welcher Kombination mehrere davon verwendet werden dürfen, trifft das Gesetz nicht. Betrachtet man den Sinn und Zweck dieser Adressierbarkeitsabfrage, so dient diese der Beauskunftung gegenüber einem (potentiellen) Absender, ob die Verfügung einer elektronischen Zustellung an einen eindeutig identifizierten Empfänger überhaupt möglich bzw zulässig ist. Da die Eindeutigkeit eines Betroffenen mit nur einem der Suchkriterien nicht in jedem Fall gewährleistet werden kann, wird davon auszugehen sein, dass die kombinierte Verwendung mehrerer Pa-

[165] Da sowohl der Zustellkopf als auch die absendende Behörde Auftraggeber iSd § 4 Z 4 DSG sind, handelt es sich bei der Antwort einer Adressierbarkeitsabfrage um eine Datenübermittlung iSd § 4 Z 12 DSG.

rameter zulässig sein wird. Da es sich bei der Übermittlung solcher Parameter an den Zustellkopf um eine Datenübermittlung iSd § 4 Z 12 DSG handelt, ist auf Grund des Wesentlichkeitsgrundsatzes gem § 6 Abs 1 Z 3 DSG zu beachten, dass bei jeder individuellen Abfrage nur die für eine eindeutige Identifikation absolut notwendigen Parameter zum Einsatz kommen dürfen. Beispielsweise kann eine natürliche Person allein durch ihren Namen nicht eindeutig identifiziert werden, da Namensgleichheiten keine Seltenheit darstellen. Hierfür ist folglich ein weiteres Identifikationsmerkmal wie Geburtsdatum oder Wohnadresse notwendig. Anders stellt sich der Sachverhalt bei Verwendung des bPK oder der SZ dar, da diese Kennnummern bereits für sich eine eindeutige Identifikation ermöglichen (vgl § 6 Abs 1 E-GovG).
Eine detaillierte Definition, welche Parameter(kombinationen) der Zustellkopf als zulässig akzeptiert, findet sich in der Spezifikation ZUSEKOPF. Diese Einschränkung geht auch mit den eben genannten datenschutzrechtlichen Anforderungen konform. Abhängig davon, ob es sich um eine natürliche oder juristische Person handelt, sind demzufolge folgende Parameter(kombinationen) zulässig[166]:

<u>Für natürliche Personen:</u>

- Verschlüsseltes oder unverschlüsseltes Zustell-bPK
- Name + Geburtsdatum
- Name + elektronische Verständigungsadresse + Geburtsdatum (optional)
- Name + physische Abgabestelle + Geburtsdatum (optional)

<u>Für juristische Personen:</u>

- Stammzahl + Typ der Stammzahl
- Bezeichnung + elektronische Verständigungsadresse
- Bezeichnung + physische Abgabestelle

Der Typ der Stammzahl legt näher fest, in welchem Register die juristische Person geführt wird (zB Firmenbuch, Vereinsregister, etc).[167] Diese Parameterkombinationen ermöglichen damit zuverlässige eindeutige Identifikation des Empfängers, berück-

[166] *Tauber/Rössler*, ZUSEKOPF, 6.
[167] ZB Firmenbuch: „FN“, ZVR: „ZVR“, ErsB: „ERSB“.

sichtigen andererseits aber auch den datenschutzrechtlichen Wesentlichkeitsgrundsatz.

7.2 Die Antwort des Zustellkopfs

Nachdem der Zustellkopf anhand der ihm übermittelten Parameter die entsprechende Abfrage in seinem Verzeichnis durchgeführt hat, generiert er daraus einen strukturierten Antwortdatensatz, welchen er der anfragenden Behörde übermittelt. Welche konkreten Parameter der Antwortdatensatz enthalten darf, ist ebenfalls in § 34 Abs 1 ZustG geregelt. Satz 2 sieht Folgendes vor: „*Liegen diese Voraussetzungen*[168] *vor, so sind die Informationen gemäß § 33 Abs. 1 Z 6 und 7*[169] *sowie die Internetadresse des Zustelldienstes, bei dem der Empfänger angemeldet ist, der Behörde zu übermitteln; andernfalls ist der Behörde mitzuteilen, dass diese Voraussetzungen nicht vorliegen.“*

Die Internetadresse des Zustelldienstes ist die Adresse jenes Webservices, an welches die zuzustellenden Dokumente von der Behörde zu übermitteln sind. Auch dafür sieht die Spezifikation eine detaillierte Schnittstellendefinition vor, um die Interoperabilität des Systems gewährleisten zu können. Diese Schnittstelle hat auch rechtliche Bedeutung, da über sie der Vertrag über die Zustellleistung abgeschlossen wird (vgl Kapitel 3.3.2).

7.3 Die technischen Voraussetzungen für die Abfrage

Im ersten Schritt, um als Behörde die Ermittlungsleistung überhaupt in Anspruch nehmen zu können, ist eine „Registrierung“ beim Zustellkopf als Versender notwendig.[170] Hierbei wird es sich um einen zivilrechtlichen Vertrag zwischen Behörde und dem EuZD handeln.[171] Diesbezügliche nähere Ausführungen erfolgen noch in Kapitel 9.

Im Zuge dieser Registrierung hat der designierte Versender dem Zustellkopf folgende Daten bekannt zu geben:

---

[168] Der Empfänger ist generell bei einem Zustelldienst angemeldet und hat die elektronische Zustellung aktuell nicht gem § 33 Abs 2 ZustG ausgeschlossen.
[169] Dies sind die akzeptierten Dateiformate und Angaben zur inhaltlichen Verschlüsselung.
[170] *Tauber/Rössler*, ZUSEKOPF, 4; http://zkopf.zustellung.gv.at/zkopf/index.jsp (Abruf: 12. 6. 2011).
[171] Vgl *Reichstädter/Rössler/Tauber*, ZUSERECH, 6 bzgl Periodizität der Rechnungslegung.

- Name der Organisation
- Kontaktadresse (physisch und elektronisch)
- Rechnungsadresse
- Zertifikat für die SSL-Verbindung

Die Rechnungsadresse ist jene Adresse, an welche der Zustellkopf im Zuge der Erbringung der *Verrechnungsleistung* (Kapitel 9) die für alle Zustelldienste akkumulierte Abrechnung für alle durchgeführten Zustellleistungen übermittelt. In welchem Intervall („Periodizität“) diese Rechnungslegung gegenüber dem Versender erfolgen soll, bedarf einer individuellen Vereinbarung.

Im Zuge dieser Registrierung ist auch ein qualifiziertes Zertifikat in Form einer Zertifikatsdatei (zB PKCS#12) zu übermitteln. Dieses Zertifikat wird im Zustellkopf hinterlegt und ist für den Aufbau einer TLS-Verbindung zwischen der Behörde und dem Zustellkopf notwendig. Ein Verbindungsaufbau zum Zustellkopf von einer Person, deren Zertifikat nicht hinterlegt ist, wird vom Server (automatisiert) verweigert. Dadurch wird technisch sichergestellt, dass nur berechtigte Personen beim Zustellkopf Adressierbarkeitsabfragen durchführen können. Der Zustellkopf kann in weiterer Folge aus diesem Zertifikat auch Identifikationsdaten auslesen, von welcher Behörde diese SSL-Verbindung aufgebaut wurde, und darauf basierend entsprechende Protokoll- und Verrechnungsdaten erzeugen. Weiters besteht auch eine Einschränkung dahingehend, welche Zertifikatsprodukte vom Zustellkopf zur Hinterlegung akzeptiert werden. Eine Liste der akzeptierten Zertifikatsprodukte findet sich auf der Homepage des Zustellkopfs[172].

Dieselbe Zertifikatsdatei ist auch bei jedem Zustelldienst zu hinterlegen, an welchen die Behörde Zustellstücke übergeben möchte. Auch die Übermittlung von zuzustellenden Dokumenten an einen Zustelldienst ist an den vorherigen Aufbau einer verschlüsselten TLS-Verbindung unter beiderseitiger Server-Authentifizierung gebunden.

[172] Aktuell werden folgende Produkte akzeptiert: a-sign-corporate-light-02, a-sign-SSL-03, a-cert-government und a-cert-advanced (http://zkopf.zustellung.gv.at/zkopf/index.jsp, 28. 5. 2011).

7.4 Der technische Ablauf einer Adressierbarkeitsabfrage

Nachdem die Behörde eine sichere TLS-Verbindung zum Zustellkopf aufgebaut hat, können über diese beliebig viele Abfragen durchgeführt werden. Für eine Anfrage an den Zustellkopf stehen aktuell zwei Varianten zur Verfügung:

- Einzelabfrage
- Bulk-Abfrage

Die Einzelabfrage ermöglicht es, die Zustellbarkeitsparameter einer einzigen Person abzufragen, die Bulk-Abfrage erlaubt dies mit einem einzigen Datensatz für eine Vielzahl von Personen.

7.4.1 Die Einzelabfrage

Im Zuge der Einzelabfrage können die Abfrageparameter direkt in der URL, mit welcher die Abfrage durchgeführt wird, übergeben werden. Am Ende der URL wird ein „?“ als Trennzeichen angehängt, welches anzeigt, dass es sich bei den nachfolgenden Zeichen um Parameter handelt. Die zulässigen Parameter werden mittels eines in ZUSEKOPF definierten „Bezeichners“ identifiziert und nach einem „=“-Zeichen wird der Wert des jeweiligen Parameters angegeben. Mehrere Parameter werden durch „&“ verbunden. Die so generierte Abfragezeichenkette bestehend aus der URL des Zustellkopfs und den entsprechenden Abfrageparametern muss noch URL-codiert werden. Das bedeutet, dass bestimmte reservierte Sonderzeichen wie zB „@“ oder „=“, denen innerhalb der URL eine spezielle Funktion zukommt, in den Abfrageparametern durch eine bestimmte zulässige Codesequenz (zB „%40“) ersetzt werden müssen.[173] Dieses Codierungserfordernis bezieht sich jedoch nur auf die Zeichenkette der Abfrageparameter selbst, da solchen Zeichen im „Rest“ der URL ja ihre zugedachte Sonderfunktion (wie beispielsweise dem „=“ die Zuweisung von Werten zu Parametern) zukommen soll.

Beispiel einer Einzelabfrage:

```
https://zkopf.zustellung.gv.at?sn=Horn&givenName=Bernhard&gvBirthdate=1980-01-01
```

[173] Vgl RFC 1738.

Werden mehrere Parameter angegeben, so müssen ALLE Parameter übereinstimmen, um zu einem positiven Ergebnis zu gelangen. Eine detaillierte Beschreibung, welche Parameter in welcher Kombination und Zeichenformatierung zulässig sind, findet sich in der Spezifikation ZUSEKOPF (vgl Kapitel 7.1).

7.4.2 Die Antwort des Zustellkopfs auf eine Einzelabfrage

Während die Abfrage durch den Zustellkopf verarbeitet wird, wartet die anfragende Applikation (also der Client) nach Absetzung des Requests auf den Erhalt der entsprechenden Response. Über diese „offene“ HTTP(S)-Verbindung wird in der Folge auch der Antwortdatensatz in Form eines XML-Containers an den Client übermittelt. Dieser Antwortdatensatz beinhaltet nun entweder einen bestimmten Fehlercode oder die vom Zustellgesetz in § 34 Abs 1 ZustG normierten Antwortdaten. Fehlercode 404 bedeutet beispielsweise, dass der abgefragte Empfänger bei keinem Zustelldienst registriert ist oder 403, dass die Anfrage mehrere Treffer ergab.

Beispiel für einen Fehlerfall (Empfänger nicht registriert):

```
<?xml version="1.0" encoding="UTF-8"?>
<StdAnswer xmlns="http://reference.egovernment.gv.at/namespaces/zustellung/kopf">
      <Error>404</Error>
</StdAnswer>
```

Trat bei der Abfrage ein Fehler auf, wird der entsprechende Fehlercode als *Error*-Element zurückgegeben.

Beispiel für einen Erfolgsfall:

```
<?xml version="1.0" encoding="UTF-8"?>
<StdAnswer xmlns="http://reference.e-government.gv.at/namespaces/zustellung/kopf">
      <Success>
            <gvZbPK>...</gvZbPK>
            <Server>
                  <ZUSEUrlID>http://...</ZUSEUrlID>
                  <MIMETypes>...</MIMETypes>
                  <X509>...</X509>
            </Server>
      </Success>
</StdAnswer>
```

Verlief die Adressierbarkeitsabfrage beim Zustellkopf positiv, übermittelt dieser einen XML-Container vom Typ *Success*, welcher ein einziges Element *<gvZbPK>* mit dem Verrechnungstoken[174] für den Zustelldienst enthält und ein oder mehrere Elemente <*Server*>, je nachdem bei wie vielen Zustelldiensten der Empfänger angemeldet ist. Jedes dieser *Server*-Elemente beinhaltet die Internetadresse des Zustelldienstes, die vom Empfänger akzeptierten Datenformate und gegebenenfalls Angaben zur inhaltlichen Verschlüsselung in Form eines X509-Zertifikats.

7.4.3 Die Bulk-Abfrage

Die Bulk-Abfrage erlaubt es, mit einem einzigen HTTP-Request in einem Schritt eine Vielzahl von Adressierbarkeitsabfragen durchzuführen. Dabei werden die einzelnen Abfragen mit den entsprechenden Abfrageparametern in eine XML-Struktur („XML-Container“) eingebettet und mittels SOAP (Simple Object Access Protocol) an den Zustellkopf zur Abarbeitung übergeben[175]. So kann eine Vielzahl von Anfragen („Querys“) in einen einzigen Request verpackt werden, was aus Performancegründen vorteilhaft ist. Jede einzelne Abfrage („Query“) in einem solchen XML-Container kann – bei 0 beginnend – mit einer eindeutigen Identifikationsnummer („ID“) versehen werden, damit die entsprechenden Antwortdatensätze den einzelnen Anfragequerys zugeordnet werden können. Dies ist gemäß Spezifikation aber nicht Pflicht[176], da sich die Zuordnung zwischen Query und Query-Antwort auch aus der Reihenfolge der Elemente im XML-Container ergibt.

Zur Veranschaulichung ein kurzes Beispiel einer Abfrage einer natürlichen und juristischen Person unter Angabe eines bPK bzw einer Stammzahl:

```
<?xml version="1.0" encoding="UTF-8"?>
<BulkQuery xmlns="http://reference.e-government.gv.at/namespaces/zustellung/kopf">
	<Query ID="0">
		<gvZbPK>8ade234abfeaf92sf02ad3ef9d86ce14a12e==</gvZbPK>
	</Query>
	<Query ID="1">
		<gvZbPK>123456x</gvZbPK>
	</Query>
</BulkQuery>
```

[174] Dieser beinhaltet seinerseits das bPK oder die SZ und dient somit ua der eindeutigen Identifizierung des Empfängers.

[175] *Tauber/Rössler*, ZUSEKOPF, 15.

[176] In der XML-Schema-Datei „zkopf.xsd“ wird diese ID mit <xs:attribute name="ID"/> spezifiziert, wobei kein „use“-Attribut (use=“required“) angegeben ist und daher ein solches Element standardmäßig optional ist.

7.4.4 Die Antwort auf eine Bulk-Abfrage

Die Struktur der Antwort des Zustellkopfs auf eine Bulk-Abfrage gestaltet sich im Wesentlichen gleich zur Einzelabfrage, nur mit dem Unterschied, dass hier entsprechend der Anzahl von Querys eine Liste von Query-Antworten retourniert wird. Jede dieser einzelnen Query-Antworten besteht entsprechend der Einzelabfrage entweder aus einem *Error*-Element oder aus einem *Success*-Element.

7.5 Die Protokollierung von Zustellkopfabfragen

Wird beim Zustellkopf eine Adressierbarkeitsabfrage durchgeführt, so müssen von diesem für jede einzelne Abfrage bestimmte Protokollierungsinformationen gespeichert werden, unabhängig davon, wie das Ergebnis der Abfrage ausfällt. Erfolgt eine Abfrage in Form einer Bulk-Abfrage, so ist für jede einzelne enthaltene Abfrage (Query) die entsprechenden Protokollierungsinformationen zu speichern.

Die Spezifikation ZUSEKOPF verpflichtet zur Protokollierung folgender Informationen[177] und erfüllt gleichzeitig auch die Protokollierungspflicht gem § 14 Abs 2 Z 7 DSG:

- Datum und Zeit der Abfrage
- Identität der abfragenden Behörde[178]
- Behördliche oder privatrechtliche Zustellung?
- Fehlercode (im Fehlerfall)
- Verrechnungstoken [,Kundennummer] (im Erfolgsfall)

7.6 Die Generierung des Verrechnungstokens

Zur Erbringung der Verrechnungsleistung ist es notwendig, dass der Zustellkopf bei jeder eingehenden Abfrage, die zu einem positiven Treffer führt, ein „Verrechnungstoken“ erstellt. Dabei handelt es sich um eine Art „Briefmarke“ in Form eines genau spezifizierten Datensatzes, in welchem auch der abgefragte Empfänger eindeutig identifizierbar festgehalten wird. Dieser Verrechnungstoken wird vom Zustell-

[177] *Tauber/Rössler*, ZUSEKOPF, 25.

[178] Die Identität der anfragenden Behörde ergibt sich aus dem Zertifikat der Behörde, welches bei der „Anmeldung“ der Behörde beim Zustellkopf hinterlegt wurde und zum Aufbau der TLS-Verbindung zwischen Behörde und Zustellkopf für die beiderseitige Authentifizierung verwendet wurde. Das Zertifikat weist eine Seriennummer und die Behördenbezeichnung auf.

kopf verschlüsselt und einerseits vom Zustellkopf selbst gespeichert und andererseits in der Zustellkopfantwort im XML-Element *<gvZbPK>* an die anfragende Behörde übermittelt. Die Behörde gibt diesen Verrechnungstoken ihrerseits neben den zuzustellenden Dokumenten an den Zustelldienst weiter, welcher den Verrechnungstoken entschlüsselt und daraus das bPK bzw die Stammzahl des Empfängers extrahiert. Im Zuge der Verrechnung übermittelt der Zustelldienst die Daten aus diesem Token wiederum an den Zustellkopf, um das Entgelt für die Zustellung zu erhalten. Auf diese Weise wird sichergestellt, dass ein Zustelldienst nur tatsächlich erbrachte Zustellungen verrechnen kann, da für jeden Verrechnungsposten eine entsprechende Abfrage beim Zustellkopf protokolliert sein muss.

Im Gegensatz zur Zustellkopfanfrage beinhaltet das Element *<gvZbPK>* in der Zustellkopfantwort folglich nicht direkt das bPK bzw die SZ des Empfängers, sondern das (verschlüsselte) Verrechnungstoken, welches aber seinerseits das bPK bzw die SZ beinhaltet. Die Berechnungsvorschrift für diesen Token ist in ZUSEKOPF in Anhang A spezifiziert und muss genau eingehalten werden:

$$RSA_{pub}(Zufallstoken + :: + bPK_{ZU})$$

Im ersten Schritt wird eine beliebige 96 Bit (= 12 Byte) lange Zufallszahl, der *Zufallstoken*, generiert. Dieser Zufallstoken wird im Anschluss Base64-kodiert, um ihn von Sonderzeichen zu befreien und in eine codepage-unabhänige Darstellung zu überführen. Das Zufallstoken wird von seiner binären Darstellung somit in eine auch für den Menschen einfach lesbare Darstellung konvertiert und stellt dadurch eine Zeichenkette dar. An diese Zeichenkette werden einfach 2 Doppelpunkte und danach das bPK für den Bereich Zustellung bzw die Stammzahl je ebenfalls in Base64-codierter Form angehängt. Diese gesamte Zeichenkette wird nun mit dem öffentlichen Schlüssel jenes Schlüsselpaares verschlüsselt, welches jedem Zustelldienst im Zuge seiner Zulassung überlassen wird. Dieses Schlüsselpaar ist für alle zugelassenen Zustelldienste dasselbe und gewährleistet, dass nur berechtigte Zustelldienste durch entsprechende Entschlüsselung des Verrechnungstokens den eindeutigen Personenbezug herstellen können.[179] De facto wird hier ein asymmetrisches Verschlüsselungsverfahren symmetrisch verwendet.

[179] Vgl *Tauber/Rössler*, ZUSEKOPF, 5.

Diese Systematik erscheit auf den ersten Blick unnötig kompliziert, realisiert aber eine wichtige Datensicherheitsmaßnahmen und ein 4-Augen-Prinzip. Zum einen ist dadurch gewährleistet, dass nur ein zugelassener Zustelldienst das Verrechnungstoken, das er von der Behörde für die Durchführung der Zustellung erhalten hat, entschlüsseln und so den Empfänger eindeutig identifizieren kann. Andererseits kann ein Zustelldienst auch faktisch nur Zustellungen verrechnen, für die er tatsächlich von einer Behörde beauftragt wurde, da er anderenfalls nicht über ein gültiges Verrechnungstoken (respektive die Zufallszahl aus dem Token) verfügen würde. Der Zustellkopf überprüft nämlich im Zuge der Verrechnungsleistung, ob für jede von einem Zustelldienst verrechnete Zustellung auch eine korrespondierende Abfrage einer Behörde protokolliert ist. So können unberechtigte Verrechnungen oder Doppelverrechnungen ausgeschlossen werden. Aus diesem Grund ist es auch notwendig, dass der Zustellkopf sämtliche Abfragen protokolliert und die von den Zustelldiensten übermittelten Verrechnungsdaten mit diesen protokollierten Abfragen abgleicht.

8. Die Zustellleistung

Die eigentliche Ausführung des Zustellvorgangs gem § 3 ZustG erfolgt bei der elektronischen Zustellung durch Erbringung der Zustellleistung (§ 29 Abs 1 ZustG). Die Zustellleistung ist von jedem zugelassenen Zustelldienst zu erbringen und umfasst entsprechend der Ziffern folgende Leistungen:

1) Die Aktualisierungsleistung (vgl Kapitel 6)
2) Die Implementierung einer technischen Schnittstelle zur Entgegennahme von zuzustellenden Dokumenten gemäß der Zustellspezifikation ZUSEMSG[180]
3) Betrieb der technischen Infrastruktur zur Bereithaltung zuzustellender Dokumente für den Empfänger
4) Die Verständigung des Empfängers über das Bereitliegen eines Dokuments
5) Die (verschlüsselte) Speicherung zuzustellender Dokumente
6) Die Bereitstellung eines Verfahrens zur qualitätsvollen Abholung zuzustellender Dokumente durch den Empfänger
7) Die Protokollierung der erfolgten Verständigungen und die Abholung des Dokuments sowie die Übermittlung dieses Zustellnachweises an die Behörde

[180] *Rössler/Tauber/Reichstädter*, Elektronische Zustellung – Message Spezifikation.

8) Die unverzügliche Verständigung der Behörde, wenn ein Dokument innerhalb der 2wöchigen Bereithaltefrist nicht abgeholt wurde
9) Die Beratung von Empfängern (zB Hotline)
10) Auf Verlangen des Empfängers die (postalische) Übermittlung des zuzustellenden Dokuments auf einem Datenträger oder eines Ausdrucks dessen in Papierform
11) sofern der Zustelldienst diese Leistung anbietet, die Weiterleitung eines zuzustellenden Dokuments an den Elektronischen Rechtsverkehr der Gerichte (ERV, §§ 89a ff GOG)

Für die Erbringung der Leistungen 1 – 9 muss die Behörde das Entgelt leisten, dessen Höhe sich für alle zugelassenen Zustelldienste aus dem Vertrag ergibt, der zwischen BK und EuZD auf Basis der Ausschreibung gem § 32 Abs 1 ZustG geschlossen wurde. Nimmt ein Empfänger die Leistung gem Punkt 10 in Anspruch, so muss er das dafür fällige Entgelt, welches sich aus dem Leistungsverzeichnis des Zustelldienstes und den im Zuge des Zulassungsverfahrens genehmigten AGB[181] ergibt, selbst bezahlen. Für die Leistung gem Punkt 11 wurde eine entsprechende Entgeltregelung offenbar übersehen.

8.1 Die Übergabe von zuzustellenden Dokumenten

Damit eine Behörde Dokumente, die dem Empfänger im Zuge einer elektronischen Zustellung zugestellt werden sollen, dem Zustelldienst übergeben kann, muss dieser eine entsprechende standardisierte Schnittstelle zur Verfügung stellen, über welche die Dokumente entgegengenommen werden können. Dadurch kann eine schnelle und kostengünstige Anbindung einer Behörde an mehrere oder alle Zustelldienste geschaffen werden, da seitens der Behörde nicht unterschiedliche Schnittstellendefinitionen implementiert werden müssen. Eine genaue Definition dieser Schnittstelle findet sich in der Spezifikation ZUSEMSG.

Die Übergabe der zuzustellenden Dokumente an den Zustelldienst erfolgt über SOAP with Attachments (SwA)[182], bei welchen die zuzustellenden Dokumente neben den Metainformationen unmittelbar mit übermittelt werden, oder über „einfache“ SO-

[181] § 30 Abs 1 ZustG.
[182] Vgl http://www.w3.org/TR/SOAP-attachments, abgerufen am 17. 1. 2011.

AP-Nachrichten, die lediglich eine Referenz auf die zuzustellenden Dokumente bei der Behörde (als Absender) beinhalten. Im zweiten Fall muss der Zustelldienst die zuzustellenden Dokumente mittels eines „Callbacks“ selbst vom Server der Behörde nachladen. Die entsprechenden Dateien zur Definition dieser Schnittstellen befinden sich ebenfalls in der Spezifikation und sind normativer Bestandteil[183]. SOAP basiert auf XML zur Repräsentation von Daten und Funktionsaufrufen und ermöglicht es, Daten zwischen zwei Computersystemen auszutauschen oder Funktionen anderer Computersysteme aufzurufen. Eine SOAP-Nachricht besteht aus einem SOAP-Envelope, das obligatorisch einen SOAP-Body enthalten muss; fakultativ kann auch ein SOAP-Header eingebettet werden. Über welches Protokoll (zB FTP, SMTP, HTTP) die SOAP-Nachricht im Endeffekt über das Internet transportiert wird, ist nicht weiter relevant. Die Spezifikation beschreibt detailliert, welche konkreten Daten im Zuge einer Ablieferung eines zuzustellenden Dokuments innerhalb der SOAP-Nachricht übermittelt werden müssen und wie die Datenstruktur solcher Nachrichten aussehen muss. Weiters ist auch geregelt, wie und in welcher Form die zuzustellenden Dokumente (als Attachments) an den Zustelldienst zu übergeben sind.

Prinzipiell erfolgt die Dokumentenanlieferung beim Zustelldienst über MIME-Nachrichten. Bei MIME (Multipurpose Internet Mail Extensions) handelt es sich um einen Standard, der Struktur, Aufbau, Typ und Kodierung von (binären) Daten festlegt, die eingebettet in Textnachrichten (zB per E-Mail[184]) übertragen werden sollen. Der Standard ermöglicht es, dass innerhalb einer Textnachricht bestimmte „Blöcke“ definiert werden können, wobei jeder dieser Blöcke unterschiedlichen (binären) Inhalt aufnehmen kann (zB Text, Bilder, Musik, proprietäre Dateien). Zu jedem Block ist weiters der Typ der beinhalteten („gekapselten“) Daten und deren Kodierung anzugeben („Mulit-part MIME-Messages“). Bei dieser Typangabe handelt es sich um dieselbe Technologie wie bei der Definition der akzeptierten Dateiformate durch den Empfänger behördlicher Dokumente (vgl Kapitel 4.1.5). Auf diese Art und Weise können beliebige Dateien als „Attachments“ in eine Textnachricht eingebettet werden. Dateien, die nicht aus reinem Text bestehen, müssen in eine andere Kodierung überführt werden, sodass sie als reiner Text in die Textnachricht aufgenommen wer-

[183] § 3 Abs 1 Z 7 ZustDV.

[184] Für E-Mail-Anhänge ist dies beispielsweise notwendig, da mit dem Protokoll SMTP lediglich Textnachrichten übertragen werden können und binäre Daten somit auf eine bestimmte Art und Weise codiert in die Textnachricht eingebettet werden müssen.

den können. Dies erfolgt durch Base64-Kodierung[185], wobei es sich dabei um ein Verfahren handelt, mit welchem beliebige Daten so konvertiert werden, dass sie nur mehr durch die Zeichen `A-Z, a-z, 0-9, +` und `/` sowie `=` am Ende repräsentiert werden. Dadurch wird jede beliebige Binärdatei sozusagen auch für den Menschen lesbar und beinhaltet keine Sonderzeichen mehr, wodurch sie in jede beliebige Textdatei eingebettet werden kann. Darüber hinaus ist auch gewährleistet, dass Kompatibilitätsprobleme auf Grund der Verwendung verschiedener Codepages beim Sender und Empfänger vermieden werden können. Bei Codepages handelt es sich um länder- bzw sprachspezifische Zeichensätze.

Auch die SOAP-Nachricht, welche neben den Zustelldokumenten auch die zu übermittelnden Metadaten beinhaltet, wird einfach als solcher Block („MIME-part“) in Form einer Textnachricht übermittelt. Wie oben dargelegt, können die zuzustellenden Dokumente nun direkt in die an den Zustelldienst zu übergebende Nachricht als MIME-parts in Base64-kodierter Form eingebettet werden oder es werden eben nur entsprechende Referenzen übergeben, die auf die bei der Behörde (über das Internet zugänglich) verfügbar gehaltenen Zustelldokumente verweisen (Callback).

Das nachfolgende Beispiel einer solchen Textnachricht ist ZUSEMSG entnommen. Der Typ der Nachricht ist `multipart/mixed`, da mehrere Datenblöcke mit unterschiedlichen Datenformaten enthalten sind (konkret reiner Text und eine PDF-Datei). Die „Grenze“ zwischen den einzelnen Blöcken („MIME-parts“) kann beliebig mit `boundary` definiert werden. Im Anschluss befinden sich nacheinander die einzelnen Datenblöcke getrennt durch die definierte Begrenzungszeichenkette und zu jedem dieser Datenblöcke die Art der beinhalteten Daten (zB `application/pdf` für ein PDF-Dokument).

Beispiel für eine solche Textdatei im Multipart-MIME-Format[186]:

```
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="-------------070603060700010608080604"
This is a multi-part message in MIME format.
```

[185] RFC 4648.
[186] *Rössler/Tauber/Reichstädter*, Message Spezifikation, 7.

```
-------------070603060700010608080604
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
Das ist eine elektronische Zustellung!
-------------070603060700010608080604
Content-Type: application/pdf; name="test.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="test.pdf"
PHA+TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQgY29uc2VjdGV0dWVyIGNvbnNlcX
....
-------------070603060700010608080604
```

Hat nun der Empfänger Daten zur Verschlüsselung bei seinem Zustelldienst hinterlegt, so muss die Behörde die zuzustellenden Daten vor Übermittlung an den Zustelldienst verschlüsseln (§ 34 Abs 1 ZustG). Dafür muss die gesamte Textnachricht, wie sie ansonsten in unverschlüsselter Form an den Zustelldienst übergeben worden wäre, verschlüsselt und in eine CMS-Datei[187] eingebettet werden.

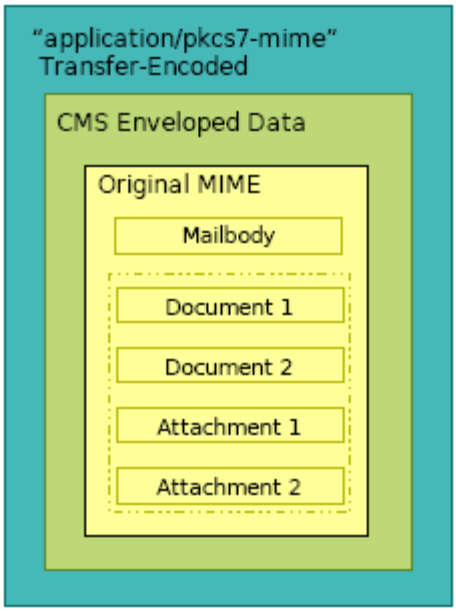

Abbildung 10: Container-Struktur einer verschlüsselten Zustellung[188]

Diese verschlüsselte CMS-Datei wird ihrerseits in Base64-kodierter wiederum in einen MIME-Container eingebettet. Diese MIME-Textdatei ist nun jedoch vom Typ Sin-

[187] Cryptographic Message Syntax, RFC 5652.
[188] *Rössler/Tauber/Reichstädter*, ZUSEMSG, 9.

gle-Part, da sie nur mehr einen Block mit der CMS-Datei beinhaltet. Der Typ dieser Nachricht ist nun `application/x-pkcs7-mime` und die Kodierung wiederum Base64. An diesem Typ der Nachricht erkennt der Empfänger (bzw dessen Software) nun, ob es sich um eine unverschlüsselte oder verschlüsselte Datei handelt. Ggf nach Entschlüsselung können nun die entsprechenden Nachrichteninhalte sowie Dokumente aus der erhaltenen Textdatei extrahiert, eventuelle Kodierungen dekodiert und die Dokumente auf Grund der Typangabe wieder in ihre binäre Form konvertiert werden.

Neben den zuzustellenden Dokumenten müssen auch bestimmte Daten an den Zustelldienst zur Durchführung der Zustellung übergeben werden. Diese werden ebenfalls innerhalb der SOAP-Nachricht als Metadaten übermittelt, welche ihrerseits einfach als Block in die Mulitpart-MIME-Textnachricht eingebettet werden. Detaillierte Informationen, welche Daten Pflichtangaben sind und welche fakultativ übermittelt werden können, finden sich in ZUSEMSG. Die wichtigsten Metadaten sind zusammengefasst: Identifikationsnummern des zuzustellenden Dokuments, Absender, Empfänger (Verrechnungstoken), Zustellqualität (hier ist auch anzugeben, ob die Abholung durch Ersatzempfänger zulässig ist; vgl §§ 35 Abs 3 ZustG, 5 E-GovG), die Benachrichtigungsadresse des Absenders, an die der Zustellnachweis übermittelt werden soll (zB URL eines Webservices, Adresse bei einem Zustelldienst, E-Mail-Adresse) und der Zeitpunkt, ab welchem die erste Verständigung des Empfängers bezüglich des Vorliegens eines Zustelldokuments erfolgen muss.[189] Darüber hinaus können noch eine Vielzahl weiterer Parameter zum Einsatz kommen, die Notwendigkeit deren Verwendung hängt jedoch davon ab, welches Leistungsangebot der Zustelldienst bereitstellt.

Nachdem ein Zustellstück an den Zustelldienst übergeben wurde, übersendet dieser für jedes übergebene Zustellstück eine entsprechende separate Erfolgs- oder Fehlernachricht. Bei einer Übergabe der Zustellstücke mittels Callback erfolgen (im Erfolgsfall) zwei Notifikationen: die eine beim Erhalt der Multipart-MIME-Textnachricht und mit der zweiten kündigt der Zustelldienst dem Behördenserver gegenüber an, dass Attachments nachgeladen werden.

[189] Vgl *Rössler/Tauber/Reichstädter*, ZUSEMSG, 10 ff.

8.2 Abholung des Dokuments und Zustellnachweis[190]

Möchte nun ein Empfänger ein für ihn beim Zustelldienst bereit liegendes Dokument abholen, muss der Zustelldienst sicherstellen, dass solche Dokumente tatsächlich nur von jener Person abgeholt werden können, für welche sie auch bestimmt sind (§ 35 Abs 3 ZustG). Allenfalls kann eine Abholung auch durch einen Ersatzempfänger erfolgen, sofern die Behörde eine Zustellung an (bzw Abholung durch) einen solchen durch entsprechende Angabe in der Zustellqualität nicht ausgeschlossen hat. Eine solche Zustellbevollmächtigung ist als „Spezialvollmacht" gem § 5 E-GovG in die Bürgerkarte des Vertreters einzutragen. Prinzipiell muss eine Abholung von Dokumenten immer unter Verwendung der Bürgerkarte erfolgen (§ 35 Abs 3 ZustG). Gegebenenfalls kann eine Abholung auch durch den Einsatz automatisiert ausgelöster Signaturen erfolgen, sofern dafür eine sichere Technik zum Einsatz kommt (zB Einbindung eins Softwarezertifikats in die Mailclient-Software). Details dazu finden sich in der Spezifikation ZUSEMAIL[191].

Der Zeitpunkt der Abholung ist vom Zustelldienst zu protokollieren, ebenso wie die Zeitpunkte der vorangegangenen Verständigungen über das Bereitliegen von Dokumenten an die bekannt gegebene elektronische Adresse und ggf an die physische Abgabestelle. Um die Akzeptanz des Verfahrens bei den (potentiellen) Empfängern zu erhöhen, muss nicht die Übernahme jeder einzelnen Nachricht digital signiert werden, sondern es gelten alle zum Zeitpunkt des Logins bereitgehaltenen Dokumente mit diesem Zeitpunkt als zugestellt. Dem Empfänger wird somit im Zuge der Abholung der Dokumente lediglich ein bestimmter Text zur Signierung vorgelegt, mit welchem er die Übernahme sämtlicher vorliegender Dokumente bestätigt („Authblock"). Daraus resultiert die Regelung, dass Dokumente auch nach Ablauf der Abholfrist noch 2 Wochen bereitgehalten werden müssen (§ 35 Abs 4 ZustG), um eventuellen Problemen beim Download der Dokumente zu begegnen.
Der Authblock muss jedenfalls folgende Informationen beinhalten[192]:

1. Name
    a. natürliche Person: Name des Empfängers

[190] *Rössler/Tauber/Reichstädter*, ZUSEMSG, 24 f.
[191] *Posch/Rössler*, Elektronische Zustellung – Abholung von Zustellung über E-Mail-Clients.
[192] *Tauber/Rössler/Reichstädter*, ZUSESPEC, 13.

   b. juristische Person: Name und zusätzlich der Name des Vertreters
2. Geburtsdatum
   a. natürliche Person: Geburtsdatum des Empfängers
   b. juristischen Person: Geburtsdatum des Vertreters
3. Aktuelles Datum und Uhrzeit
4. URI des Zustelldienstes
5. fakultativ das verschlüsselte Zustell-bPK

Der Authblock wird zum Zeitpunkt der Abholung für alle bereitliegenden Dokumente generiert und stellt eine XML-Struktur dar, in welche die entsprechenden Zustellinformationen eingebettet werden. Der Authblock beinhaltet somit Textteile, welche dem Benutzer im Zuge des Signaturvorgangs von der BKU angezeigt werden, und weitere für diesen unsichtbare Teile. Der Authblock muss im Anschluss vom Empfänger unter Verwendung seiner Bürgerkarte digital signiert werden, wodurch der Zugang der Dokumente rechtsverbindlich bestätigt wird. Diese digitale Signatur bildet für den Abholvorgang gleichzeitig auch den Nachweis der Identität und Authentizität.

Zusammen mit den Protokolldaten bezüglich der Zeitpunkte der erfolgten Verständigungen und den folgenden weiteren Daten bildet der Authblock den Zustellnachweis. Ein solcher Zustellnachweis muss für jedes einzelne Dokument unter (redundanter) Einbettung des Authblocks erstellt werden und ist vom Zustelldienst seinerseits digital zu signieren[193]:

1. Zustelldienst
2. Kennummern des Zustellstücks
3. Protokollinformationen über erfolgte Benachrichtigungen und ggf Abholung
4. Angaben zum Absender
5. Angaben zum Empfänger
6. Erfolgsinformation
   a. Authblock einschließlich Abholzeitpunkt
   b. Information über die Nichtabholdung durch den Empfänger
7. Digitale Signatur des Zustelldienstes

[193] *Rössler/Tauber/Reichstädter*, ZUSEMSG, 22 f.

Werden die bereitliegenden Dokumente nicht innerhalb der 2wöchigen Bereithaltefirst abgeholt, so ist im Zustellnachweis anstelle des Authblocks der entsprechende Hinweis über die Nichtabholung (und nahe liegender Weise ohne den Zeitpunkt der Abholung) einzufügen und ebenfalls vom Zustelldienst digital zu signieren. Die bereitgehaltenen Dokumente sind unverzüglich zu löschen (§ 35 Abs 4 2. Satz ZustG).

Der Zustellnachweis ist unverzüglich („ehest möglich“) an jene Adresse der Behörde zu übermitteln, welche diese im Zuge der Zustellstückanlieferung angegeben hat (§§ 29 Abs 1 Z 7 und 8, 35 Abs 3 lS ZustG). Erfolgt die Übermittlung des Zustellnachweises an ein Webservice, so ist der Empfang von diesem zu bestätigen.[194]

9. Die Verrechnungsleistung

Die letzte ausdrücklich im Zustellgesetz angeführte Leistung ist die *Verrechnungsleistung* (§ 29 Abs 2 Z 3 ZustG). Das Gesetz versteht darunter „*die Weiterleitung des von den Behörden für eine Zustellung entrichteten Entgelts an jene Zustelldienste, die die Zustellleistung erbracht haben, sowie die Verrechnung der weitergegebenen Entgelte mit den Behörden“.* Nähere gesetzliche Rahmenbedingungen, wie diese Leistungen konkret zu erbringen sind, finden sich im Zustellgesetz nicht. Konkretisierende technische Anforderungen, die vom Zustellkopf erfüllt werden müssen, um diese Leistung entsprechend dem Stand der Technik (§ 29 Abs 1 ZustG) zu erbringen, werden in der Spezifikationen ZUSERECH normiert.

9.1 Das Entgelt für die Verrechnungsleistung

Für die Erbringung der Verrechnungsleistung hat der EuZD Anspruch auf Entgelt, das von derjenigen Behörde zu leisten ist, für welche die Verrechnungsleistung erbracht wird (§ 29 Abs 2 aE ZustG). Ob dieser Anspruch gesetzlicher oder vertraglicher Natur ist, geht aus dem Gesetz nicht explizit hervor. Analog zur Erbringung der Zustellleistung wird es sich bei dem Rechtsverhältnis zwischen Behörde und EuZD in Bezug auf die Erbringung der Verrechnungsleistung wohl ebenfalls um ein vertragliches Schuldverhältnis handeln. Die Höhe dieses Entgelts ergibt sich analog zur Zustellleistung aus dem Ausschreibungsverfahren gem § 32 Abs 1 ZustG. So lange noch kein Ausschreibungsverfahren durchgeführt wurde, müssen die Leistungen des § 29 Abs 2 ZustG vom BKA als „Übergangszustelldienst“ kostenlos erbracht werden

[194] Vgl *Rössler/Tauber/Reichstädter*, ZUSEMSG, 24 f.

(§ 32 Abs 2 ZustG). Eine direkte Verrechnung der Zustellentgelte mit den jeweiligen Behörden durch die Zustelldienste wird wohl nicht zulässig sein, da sowohl das ZustG als auch die Zustellspezifikation die Durchführung der Verrechnung verpflichtend über den EuZD vorsehen.

Da einzig und allein der EuZD die Verrechnungsleistung erbringen darf[195], kommt diesem im gesamten Zustellsystem eine Monopolstellung[196] zu, was bei Annahme einer vollständigen Vertragsabschlussfreiheit dazu führen würde, dass dieser Behörden willkürlich von einer Teilnahme an der elektronischen Zustellung ausschließen könnte. Analog zu den „einfachen" Zustelldiensten wird folglich auch der EuZD bei der Erbringung seiner Leistungen gegenüber jedermann einem Kontrahierungszwang unterliegen (vgl Kapitel 3.3.4). Diese Annahme lässt sich auch durch das Zustellgesetz untermauern (§ 29 Abs 2): *„Einer der Zustelldienste hat außerdem folgende Leistungen zu erbringen: […]"*. Auch hinsichtlich der Erbringung dieser Leistungen werden sich mangels konkreter gesetzlicher Regelungen die *üblichen Bedingungen* für alle Behörden aus dem zwischen BK und EuZD im Zuge des Vergabeverfahrens abgeschlossenen Vertrag ergeben.

9.2 Die Übermittlung von Verrechnungsdaten

ZUSERECH sieht vor, dass jeder Zustelldienst in periodischen Abständen seine Verrechnungsdaten bezüglich aller seit der letzten Meldung durchgeführten Zustellungen an den Zustellkopf melden muss. Der Zustellkopf muss dafür eine entsprechende Schnittstelle zur Verfügung stellen, über die jeder zugelassene Zustelldienst solche Daten übermitteln kann. Die Spezifikation dieser Schnittstelle ist Teil der Zustellspezifikation (*zuserech.xsd*), wobei die Schnittstelle nur von zugelassenen Zustelldiensten genutzt werden darf. Die Übermittlung der Verrechnungsdaten erfolgt mittels SOAP über eine SSL-Verbindung.

Die Periodizität dieser Übermittlungen muss „laut unterfertigter Vereinbarung"[197] erfolgen, was ebenfalls auf die Notwendigkeit zivilrechtlicher Vereinbarungen zwischen den Zustelldiensten und dem EuZD bezüglich der Verrechnungsleistung schließen lässt. Die Nutzung dieser Schnittstelle muss den Zustelldiensten jedoch kostenfrei

[195] § 29 Abs 2 ZustG, „Einer".
[196] Vgl *Zankl*, Bürgerliches Recht, RZ 52.
[197] *Reichstädter/Rössler/Tauber*, ZUSERECH, 8.

ermöglicht werden, da nur gegenüber der Behörde ein Entgelt für die Erbringung der Verrechnungsleistung verlangt werden darf (§ 29 Abs 2 aE).

Zusammen mit den zuzustellenden Dokumenten erhält der Zustelldienst von der Behörde auch den Verrechnungstoken (vgl Kapitel 7.6), den die Behörde ihrerseits vom Zustellkopf im Zuge der Adressierbarkeitsabfrage erhalten hat. Diesen Token kann der Zustelldienst in der Folge entschlüsseln, das bPK bzw die SZ extrahieren und so den Empfänger der zuzustellenden Dokumente eindeutig identifizieren. Die Verrechnungsdaten, die jeder Zustelldienst nun an den Zustellkopf übermitteln muss, entsprechen den Protokollierungsdaten über die erbrachten Zustellungen. Diese Protokollierungsdaten umfassen (analog zur Protokollierungspflicht des Zustellkopfs im Zuge der Erbringung der Ermittlungsleistung) folgende Informationen[198]:

- Datum und Zeit der Zustellung
- Identität der abfragenden bzw zustellenden Behörde mittels der Seriennummer des Zertifikats[199]
- Verschlüsselter Verrechnungstoken
- Zustellqualität
- Bei Privatzustellung auch das Verrechnungsprofil

Aus dieser Auflistung ist erkennbar, dass von jedem Zustelldienst immer der gesamte verschlüsselte Verrechnungstoken zu protokollieren ist. Der Zustelldienst muss diesen für die Zuordnung der zuzustellenden Dokumente zum entsprechenden Empfänger zwar entschlüsseln und das bPK bzw die SZ extrahieren, für die Verrechnung muss dem Zustellkopf jedoch das unveränderte (verschlüsselte) Verrechnungstoken übergeben werden. Der Zustellkopf ermittelt in der Folge, ob zu diesem Verrechnungstoken (respektive der Zufallszahl *eID*) und der versendenden Behörde auch korrespondierende Abfrageprotokolldaten vorliegen und vermerkt dies in seiner Datenbank. Auf Grund dieser Methodik ist es technisch möglich, dass Zustellkopfabfragen kostenlos erbracht werden können, die Verrechnung einer Zustellleistung durch

[198] *Reichstädter/Rössler/Tauber*, ZUSERECH, 9; Schnittstellenspezifikation zuserech.xsd.

[199] Die Identität der anfragenden Behörde ergibt sich aus dem Zertifikat der Behörde, welches von der Behörde beim Zustelldienst hinterlegt wurde und zum Aufbau der TLS-Verbindung zwischen Behörde und Zustelldienst für die beiderseitige Authentifizierung im Zuge der Übermittlung des zuzustellenden Dokuments verwendet wird. Dieses Zertifikat weist eine eindeutige Seriennummer auf und auch der Inhaber ist darin vermerkt.

einen Zustelldienst hingegen nur dann möglich ist, wenn einem solchen von einer Behörde auch tatsächlich (gemeinsam mit den zuzustellenden Dokumenten) ein Verrechnungstoken übergeben wurde. Auf Grund der Verschlüsselung der Verrechnungstoken durch den Zustellkopf ist es Zustelldiensten somit nicht möglich, solche Token selbst zu erzeugen, also zu fälschen.

9.3 Die Abrechnung mit den Behörden

Den zweiten Teil der Verrechnungsleistung bildet die Abrechung mit den jeweiligen Absendern, für welche Zustellleistungen erbracht wurden. Die genauen Modalitäten dieser Verrechnung einschließlich der Periodizität, in welcher diese Rechnungslegung erfolgen muss, sind in der zivilrechtlichen Vereinbarung zwischen EuZD und der jeweiligen zustellenden Behörde festzulegen. Diese Vereinbarung ist zusammen mit der „Registrierung“ der Behörde beim Zustellkopf als Versender abzuschließen.

Ist nun der Zeitpunkt gekommen, zu welchem – entsprechend der oben genannten zivilrechtlichen Vereinbarung – einer Behörde eine Abrechnung der für sie durchgeführten Zustellleistungen zu übermitteln ist, muss der Zustellkopf die Anzahl der für diese Behörde seit der letzten Abrechnung durchgeführten Zustellvorgänge ermitteln. Der Zustellkopf stellt nun durch Abgleich der von den Zustelldiensten erhaltenen Protokolldaten und den korrespondierenden eigenen Protokolldaten fest, wie viele Zustellvorgänge tatsächlich von allen Zustelldiensten für die jeweilige Behörde durchgeführt und noch nicht verrechnet wurden. Aus diesen Daten wird anschließend eine Rechnung erstellt und der jeweiligen Behörde zur Bezahlung des gesamten ausstehenden Entgelts für alle Zustelldienste übermittelt. In dieser Rechnung werden die Entgelte gesondert für die jeweiligen Zustelldienste angeführt und zusätzlich auch das Entgelt für die Erbringung der Verrechnungsleistung durch den Zustellkopf ausgewiesen. Es sind von der Behörde somit die gesamten ausstehenden Entgelte für alle Zustelldienste an den EuZD zu leisten. Der EuZD betreibt nun das Inkasso dieser Rechnung und leistet die entsprechenden Beträge an die jeweiligen Zustelldienste.

9.4 Der Ablauf der Verrechnung der Zustellleistung

Im Zusammenhang mit der Abwicklung der Verrechnungsleistung stellt sich nun die Frage, wie die Konstruktion der „Weiterleitung des von der Behörde entrichteten Ent-

gelts“ und die „Verrechnung mit den Behörden“ durch den EuZD rechtlich zu beurteilen sind. Grundsätzlich sieht § 29 Abs 2 Z 3 ZustG den Ablauf der Verrechnung streng entsprechend seines Wortlauts folgendermaßen vor:

0. (Erhalt des zu entrichtenden Entgelts von den Behörden)
1. Weiterleitung des von den Behörden entrichteten Entgelts
2. Verrechnung der weitergeleiteten Entgelte

Daraus muss geschlossen werden, dass der EuZD zuerst das von der Behörde bereits erhaltene Entgelt an die jeweiligen Zustelldienste weiterleiten muss, bevor die Verrechnung mit der Behörde erfolgen darf. Aus dieser sprachlichen Konstruktion ergibt sich, dass die Entgelte bereits an die ZD als Empfänger übergeben worden sein müssen, bevor die Verrechnung zu erfolgen hat. Daher ist der EuZD nicht verpflichtet, das Entgelt gegenüber den ZDs für die Behörden zu bevorschussen. Ihn trifft somit keine (gesetzliche) Vorleistungspflicht. Erst nachdem er das Entgelt von den jeweiligen Behörden erhalten hat und dieses an die ZDs weitergeleitet wurde, muss der EuZD den einzelnen Behörden Rechnung legen. Eine solche Rechnung kann gegebenenfalls auch eine Auflistung der Entgelte gesondert nach den einzelnen Zustelldiensten oder überhaupt einen Einzelnachweis sämtlicher durchgeführter Zustellungen beinhalten.[200]

Problematisch erscheint in diesem Zusammenhang jedoch, dass die Spezifikation ZUSERECH genau von der gegenteiligen Konstruktion ausgeht, nämlich dass die Weiterleitung der Entgelte den Abschluss des Verrechnungsprozesses nach der Rechnungslegung bildet: *„Den Abschluss dieser Phase bildet die Weiterleitung des von den Behörden/Sendern für eine Zustellung entrichteten Entgelts an die jeweiligen Zustelldienste, die die Zustellleistung erbracht haben.“*[201] Diese Ansicht ist mit dem Wortlaut des ZustG auf den ersten Blick nicht vereinbar.

9.5 Der Eintritt der Fälligkeit des Zustellentgelts

Weiters ergibt sich aus dem Zustellgesetz kein Anhaltspunkt, wann die Fälligkeit der Forderung des ZD für die Erbringung der Zustellleistung gegenüber der Behörde ein-

[200] *Reichstädter/Rössler/Tauber*, ZUSERECH, 6.
[201] *Reichstädter/Rössler/Tauber*, ZUSERECH, 8.

tritt. Da entsprechend der Materialien und der Literatur keine vertragliche Bindung zwischen diesen beiden Akteuren besteht (vgl Kapitel 3.2), kann sich diese auch nicht aus einer Parteienvereinbarung ergeben. Folglich müsste es sich dabei um ein gesetzliches Schuldverhältnis handeln, für welches auch hinsichtlich der Fälligkeit die allgemeinen Regelungen des ABGB Anwendung finden.[202] Es bedarf daher einer Fälligstellung durch den Zustelldienst als Gläubiger, die jedoch nicht willkürlich ausgeübt werden darf, sondern sich nach „Natur und Zweck der Leistung" richten muss.[203] Geht man wie in Kapitel 3.2 ausgeführt jedoch von einer zivilrechtlichen Verbindung zwischen Behörde und Zustelldienst aus, können zB in den AGB oder in einem Rahmenvertrag Regelungen bezüglich der Fälligkeit getroffen werden. In diesem Fall hätte die Rechnungslegung nur mehr deklarativen Charakter, da die Fälligkeit ja bereits auf Grund der getroffenen Vereinbarung „automatisch" eintritt (§§ 1417 1. Fall iVm 904 ABGB).

Allenfalls könnte eine Fälligstellung auch durch den EuZD als Boten, Stellvertreter oder im eigenen Namen nach erfolgter Zession als Zessionar gegenüber der Behörde im Zuge der Verrechnung der Entgelte entsprechend der privatrechtlichen Vereinbarung zwischen Zustelldienst und EuZD[204] erfolgen. Eine solche zivilrechtliche Vereinbarung wird in jedem Fall notwendig sein, da ansonsten der EuZD nicht über die Rechtsposition verfügen würde, um gegenüber Behörden Entgelte rechtsgültig fällig stellen zu können.

Von einer Konstruktion der antizipierten Rechnungsstellung – die gleichzeitig auch die Einmahnung darstellt – vor Weiterleitung der Entgelte geht offenbar auch ZUSERECH aus, doch ist diese prima facie nicht mit dem Wortlaut des ZustG vereinbar. Merkwürdig erscheint in diesem Zusammenhang auf den ersten Blick weiters, dass in ZUSERECH davon ausgegangen wird, die Periodizität der Rechnungslegung in der privatrechtlichen Vereinbarung zwischen Behörde (als Schuldner für das Entgelt der Zustellleistung) und EuZD festzulegen.[205] Der Zeitpunkt der Fälligstellung einer Forderung obliegt gemäß § 1417 2. Fall ABGB jedoch ausschließlich dem Gläubiger (oder einem Dritten in dessen Auftrag), kann aber nicht in einem Vertrag zwischen

[202] *Koziol/Welser*, Bürgerliches Recht II, 38.
[203] *Koziol/Welser*, Bürgerliches Recht II, 37.
[204] *Reichstädter/Rössler/Tauber*, ZUSERECH, 8 („laut unterfertigter Vereinbarung").
[205] *Reichstädter/Rössler/Tauber*, ZUSERECH, 6.

Schuldner (Behörde) und Drittem (EuZD) festgelegt werden. Dies wäre wiederum nur dann möglich, wenn dem EuZD von den Zustelldiensten diesbezüglich bereits rechtsgeschäftlich Stellvertretungsbefugnis eingeräumt wurde oder eine Globalzession aller Forderungen vereinbart worden wäre.

Zusammengefasst kann lediglich festgestellt werden, dass eine allgemein gültige Aussage, wann und unter welchen Umständen die Fälligkeit konkret eintritt, nicht getätigt werden kann, da dies alleine von der konkreten vertraglichen Ausgestaltung zwischen den Parteien abhängt.

9.6 Die Rechtsbeziehungen bei der Verrechnungsleistung

Juristisch sehr interessant ist in diesem Zusammenhang die Frage, in welcher rechtlichen Beziehung die einzelnen Akteure bei einer solchen zentralen Ab- und Verrechnung der Zustellentgelte stehen. Das Zustellgesetz bietet diesbezüglich keine näheren Anhaltspunkte, weswegen diese Frage nach allgemeinem Zivilrecht zu beurteilen sein wird. Da bei der Erbringung der Ermittlungs- und Verrechnungsleistung keine der Parteien mit Imperium auftritt, sind diese der Privatwirtschaftsverwaltung zuzuordnen.

Wie sich die Rechtsbeziehungen zwischen Zustelldiensten, EuZD und den Behörden konkret darstellen, hängt im Wesentlichen von den privatrechtlichen Vereinbarungen zwischen den Zustelldiensten und dem EuZD sowie dem EuZD und den Behörden ab. Jedenfalls geht auch ZUSERECH davon aus, dass sowohl zwischen den Zustelldiensten und dem EuZD[206] (a) als auch dem EuZD und den jeweiligen Behörden[207] (b) ein zivilrechtlicher Vertrag zu begründen ist und somit nicht von gesetzlichen Schuldverhältnissen zwischen diesen Parteien auszugehen ist. Die Forderungen auf Grund der durchgeführten Zustellleistungen entstehen im Verhältnis zwischen dem jeweiligen ZD und Behörde (c).

[206] *Reichstädter/Rössler/Tauber*, ZUSERECH, 6, („Der genaue Wortlaut bezgl. Abwicklung, Periodizität, … ist der (bilateralen, privatrechtlichen) Vereinbarung zu entnehmen.“).
[207] *Reichstädter/Rössler/Tauber*, ZUSERECH, 8, („in der laut unterfertigter Vereinbarung festgelegten Periodizität“).

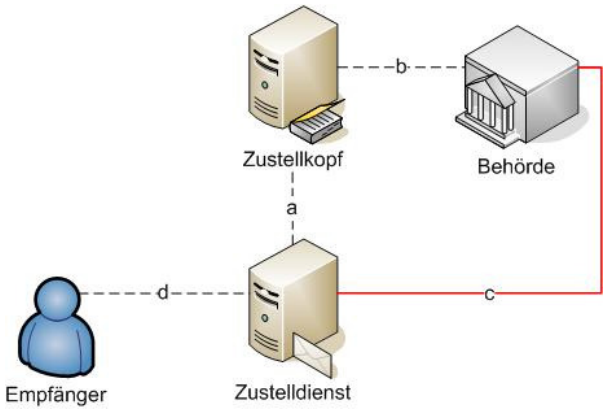

Abbildung 11: Die Rechtsbeziehungen

Im Folgenden soll nun diskutiert werden, welche zivilrechtlichen Konstruktionen dafür in Frage kommen könnten bzw welche am praktikabelsten erscheint.

9.6.1 Diskussion der Lösungsvariante mit Inkassozession

Bei den Verträgen zwischen den Zustelldiensten und dem EuZD könnte es sich um eine Globalzession aller zukünftigen Forderungen handeln, welche auf Grund der Durchführung von Zustellungen (gesetzlich oder vertraglich) begründet werden. Der Rechtsgrund der zu zedierenden Forderungen ist hier ausreichend konkretisiert, wodurch einer Globalzession theoretisch nichts im Wege steht.[208] Konkret würde es sich dabei um eine Inkassozession bzw unechtem Factoring[209] handeln, da den Behörden (als Schuldner) durch den EuZD Rechnung zu legen ist (und die Forderungen dadurch fällig gestellt würden) und das eingehobene Entgelt nach dem Inkasso an die ZDs (als Gläubiger) weiterzugeben ist. Bei diesem Vertragsverhältnis würde es sich somit um eine Treuhand handeln. Dass dem EuZD als Zessionar bzw Factor das Delkredere auferlegt werden soll, ist dem ZustG nicht zu entnehmen, jedoch wäre eine solche vertragliche Vereinbarung ebenfalls möglich. Streng genommen ist dem ZustG überhaupt nicht zu entnehmen, dass im Zuge der Verrechnungsleistung eine Zession vorgesehen ist, weswegen eine Legalzession daher jedenfalls ausscheidet.

Diese Lösung beinhaltet jedoch eine Reihe rechtlicher Probleme bzw Widersprüchlichkeiten zum Zustellgesetz und der Zustellspezifikation:

[208] *Koziol/Welser*, Bürgerliches Recht II, 127.
[209] *Koziol/Welser*, Bürgerliches Recht II, 126, 128.

- Bei der Annahme einer Inkassozession oder des Factorings würde das Vertragsverhältnis zwischen den ZD und dem EuZD ausreichend sein, zwischen EuZD und Behörden wäre ein solches nicht mehr notwendig. Dies würde aber im Widerspruch zu ZUSERECH stehen, welche auch in diesem Verhältnis von der Notwendigkeit einer vertraglichen Vereinbarung ausgeht.
- Eine solche Konstruktion würde weiters dazu führen, dass der EuZD zwar zum Inkasso der Zustellentgelte bei den Behörden aus dem Vertragsverhältnis ZD – EuZD verpflichtet wäre, ihm jedoch das Entgelt als Gegenleistung für dieses Inkasso nicht aus diesem Vertragsverhältnis zustehen würde. Dieses wäre gem § 29 Abs 2 aE ZustG ja von der Behörde zu leisten. Da ein Vertrag zu Lasten dritter zivilrechtlich nicht möglich ist, müsste es sich hinsichtlich des Verrechnungsentgelts um ein gesetzliches Schuldverhältnis zwischen Behörde und EuZD handeln. Dass es sich dabei tatsächlich um ein solches handelt, geht aus dem ZustG jedoch nicht mit Sicherheit hervor.
- Auch wenn man zusätzlich den Abschluss eines Vertrags zwischen EuZD und Behörde über die Leistung des Verrechnungsentgelts annehmen würde, würde sich auch in diesem Verhältnis wiederum ein zweiseitiger einseitig verbindlicher Vertrag ergeben, für welchen jedoch kein passender Titel erkennbar ist[210]. Auch die Notwendigkeit, dieses zweiseitige Synallagma aus Verrechnungsleistung und Verrechnungsentgelt derart auf zwei zweiseitige einseitig verbindliche Verträge aufzuspalten, erscheint wenig nachvollziehbar.
- Eine solche Inkassozession wäre weiters als Factoringgeschäft zu qualifizieren, da Forderungen aus erbrachten Dienstleistungen (der Erbringung der Zustellleistung) zediert und eingezogen werden würden. Das Factoringgeschäft ist jedoch den Banken vorbehalten (§ 1 Abs 1 Z 16 BWG), weswegen eine solche rechtliche Konstruktion von vornherein ausscheidet.

9.6.2 Diskussion der Lösungsvariante mit Auftragsrecht

Als weitaus praktikablere Lösung bietet sich jedoch die Konstruktion mit zwei **gemischten Verträgen** (vgl hierzu die Ausführungen hinsichtlich des Rechtsverhältnisses zwischen Kunde und Zustelldienst bei der Erbringung der Zustellleistung in Kapitel 3.3.1) **erweitert um Elemente des Auftragsrechts gem § 1002 ff ABGB** ohne

[210] Schenkung scheidet mangels Freizügigkeit/Zuwendungswillen aus, Auftrag mangels der Vornahme von Rechtsgeschäften/Rechtshandlungen, Werkvertrag mangels faktischer Tätigkeiten.

Forderungszession an. Dies würde auch der Intention der Spezifikation ZUSERECH entsprechen und nicht im Widerspruch zu den Regelungen des Zustellgesetzes stehen.

Die folgende Grafik stellt diese Konstruktion übersichtlich dar: Die beiden Auftragsverträge werden zwischen den Zustelldiensten und dem EuZD (a) und dem EuZD und den versendenden Behörden (b) geschlossen. Das bereits in Kapitel 3 diskutierte Schuldverhältnis für die Erbringung der Zustellleistung wird durch (c) und (d) dargestellt, wobei im Verhältnis (c) die zu tilgenden Forderungen begründet werden.

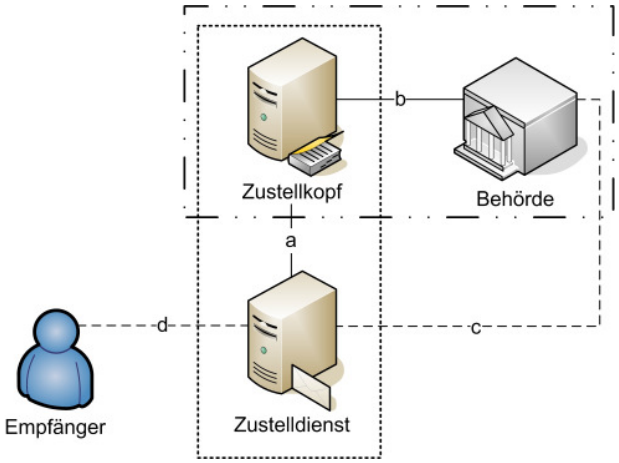

Abbildung 12: Zivilrechtliche Rechtsbeziehungen bei der Verrechnungsleistung

Das Auftragsverhältnis (a)

Im Auftragsvertrag (a) verpflichtet sich der EuZD gegenüber dem ZD zur Einmahnung und somit Fälligstellung der Entgelte für die durchgeführten Zustellvorgänge gegenüber den jeweiligen Behörden. In diesem Fall muss dem EuZD jedoch auch eine entsprechende Stellvertretungsbefugnis eingeräumt werden (§ 1008 ABGB). Im Auftragsvertrag wird nun im Innenverhältnis festgelegt, in welcher Periodizität der EuZD die Entgelte gegenüber den Behörden im Namen des jeweiligen ZDs gem § 1417 ABGB durch Übermittlung der entsprechenden in ZUSERECH festgelegten Rechnung fällig stellen darf bzw muss. Die Fälligstellung erfolgt daher durch Mahnung, wobei gewisse Periodizitäten eingehalten werden müssen. Diese Periodizität gilt es im Auftragsvertrag im Verhältnis (a) detailliert festzuhalten, wobei die eventuell im Vertrag (c) vereinbarten Fälligkeitsregelungen (zB in den AGB iSd § 29 Abs 6 ZustG) berücksichtigt werden müssen.

Eine solche Einmahnung ist an keine bestimmte Form gebunden und kann daher auch (automatisiert) per E-Mail, Fax, etc erfolgen. Sie muss als Willensmitteilung[211] dem Schuldner bloß in dessen Verfügungsmacht zugehen, um die Fälligkeit auszulösen. Diese Einmahnung ist prinzipiell unabhängig von der späteren Rechnungslegung bzw Abrechnung der weitergeleiteten Entgelte gegenüber den Behörden, da letztere ausschließlich das Vertragsverhältnis (b) betreffen. Eine solche Konstruktion wäre auch mit ZUSERECH vereinbar.

Das Auftragsverhältnis (b)

Der Auftragsvertrag (b) wird bei der jeweiligen Registrierung der Behörde als Sender beim Zustellkopf geschlossen. Der Inhalt dieses Vertrags ist die Verpflichtung des EuZD, die durch die ZD (stellvertretend durch den EuZD) fällig gestellten Forderungen für die Behörde zu begleichen und den Eintritt von Schuldnerverzug bei der Behörde zu verhindern. Der EuZD würde diesbezüglich auf fremde Rechnung für die Behörde handeln, ob diesem auch Stellvertretungsbefugnisse eingeräumt werden, obliegt der Ausgestaltung des Auftragsvertrags zwischen Behörde und EuZD. Auch eine Doppelvertretung wäre rechtlich nicht weiter problematisch, da dem EuZD ohnedies wenig bis keine wirtschaftliche Dispositionsfreiheit zukommt und auch das Entgelt fixiert ist, weswegen keine Gefährdung der Interessen der beiden vertretenen Parteien zu erkennen ist.[212]

Der Gewalthaber (EuZD) wäre somit verpflichtet, die Interessen des Gewaltgebers (Behörde) in der Form zu wahren, dass die fälligen Zustellentgelte rechtzeitig ohne Auslösung von Verzugsfolgen beglichen werden, die erlangten Vorteile herausgegeben werden (§ 1009 ABGB) und dem Gewalthaber zur gehörigen Zeit Rechnung gelegt wird (§ 1012 ABGB). Die Periodizität dieser Pflicht zur Rechnungslegung ergibt sich ausschließlich aus dem Auftragsvertrag (b) und ist unabhängig von der Einmahnung aus dem Auftragsverhältnis (a). Der Gewalthaber hat gegenüber dem Gewaltgeber das Recht, die zur Besorgung des Geschäfts notwendigen und nützlichen Aufwendungen ersetzt zu bekommen und für die Bestreitung von Barauslagen einen entsprechenden Vorschuss zu erhalten (§ 1014 ABGB). Unter solchen Barauslagen werden wohl auch jene Entgelte zu verstehen sein, welche dem jeweiligen Zustell-

[211] *Bydlinski*, Bürgerliches Recht I[5], RZ 4/14.
[212] *Koziol/Welser/Kletecka*, Bürgerliches Recht I[13], 215 f.

dienst zu leisten („weiterzuleiten“) sind und über die dem Gewaltgeber (Behörde) im Anschluss Rechnung zu legen ist (§§ 29 Abs 2 Z 3 ZustG, 1012 ABGB). Auch die Annahme dieses Auftragsvertrags (b) geht mit ZUSERECH konform, welche ebenfalls (ohne nähere Konkretisierung) von einer privatrechtlichen Vereinbarung zwischen EuZD und Behörde ausgeht[213].

9.6.3 Die Verrechnung der Verrechnungsleistung

Mit dieser Konstruktion klärt sich nun auch die Frage, auf welcher Rechtsgrundlage die Verpflichtung der Behörde zur Leistung des Entgelts für die Erbringung der Verrechnungsleistung beruht (§ 29 Abs 2 lS ZustG). Diese ergibt sich aus dem entgeltlichen Auftragsvertrag (b). Dadurch können die rechtlichen Unsicherheiten vermieden werden, die sich aus der Annahme eines gesetzlichen Schuldverhältnisses im Verhältnis (b) ergeben würden, da in diesem Auftragsvertrag detaillierte Regelungen bezüglich der Modalitäten zur Leistung des Verrechnungsentgelts getroffen werden können. Weiters ergibt sich die Höhe des Entgelts aus dem Ausschreibungsvertrag zwischen EuZD und dem BKA gem § 32 Abs 1 ZustG als eine der *üblichen Bedingungen*, zu welchen der Vertrag mit jeder Behörde unter Kontrahierungszwang abzuschließen ist (vgl Kapitel 9.1).

9.7 Wechsel des Zustellkopfbetreibers

Ein für die Praxis und vor allem für die Kontinuität der Verfügbarkeit des Zustellsystems nicht zu unterschätzendes Problem ist jener Fall, in welchem der Betrieb des Zustellkopfes von einer juristischen Person als Betreiber auf eine andere übertragen werden muss. Besonders deutlich zeigt sich dies in jenem Fall, in welchem beispielsweise dem EuZD gem § 30 Abs 4 ZustG die Zulassung entzogen wird und dieser – zB auf Grund gravierender datenschutztechnischer Mängel – unverzüglich den gesamten Betrieb einstellen muss. In diesem Fall müssten die Ermittlungs- und Verrechnungsleistung gem § 32 Abs 2 ZustG wieder vom BKA als Übergangszustelldienst erbracht werden. Die Übertragung der technischen Funktionalität wird in der Praxis möglicherweise rasch vonstatten gehen, indem der Server oder die Virtuelle Maschine (technisch unverändert) einfach beim neuen Betreiber in Betrieb genommen wird und die URL einfach auf die IP-Adresse des neuen Betreibers referenziert wird. Aus rechtlicher Sicht müssen für die Erbringung der Ermittlungs- und Verrech-

[213] *Reichstädter/Rössler/Tauber*, ZUSERECH, 6.

nungsleistung jedoch alle Verträge zwischen Behörden und EuZD sowie dem EuZD und den anderen (einfachen) Zustelldiensten entsprechend neu geschlossen werden, da nun ein anderer Rechtsträger dieselben Leistungen erbringt. Bis alle diese Verträge wieder „unter Dach und Fach" sind, kann die elektronische Zustellung nicht entsprechend in Anspruch genommen werden. Eventuell könnte ein solcher Bruch der Serviceverfügbarkeit und der dadurch entstehende administrative Aufwand doch die eine oder andere Behörde von der weiteren Nutzung des elektronischen Zustellsystems abbringen.

Eventuell wäre es sinnvoll, für diesen Fall eine Regelung in das Zustellgesetz aufzunehmen, auf Grund welcher ein neuer Betreiber bezüglich der Erbringung der Ermittlungs- und Verrechnungsleistung per Gesetz in die Rechtsverhältnisse des bisherigen Betreibers eintritt. Dies wäre vor allem für den Fall vorteilhaft, in welchem der Zustellkopf von einem kommerziellen Betreiber – aus welchem Grund auch immer und sehr wahrscheinlich aus gegebenem Anlass möglichst rasch – möglichst unterbrechungsfrei wieder zum BKA und somit in ein behördliches Umfeld „zurückgeholt" werden muss. Die „Auslagerung" vom BKA im Zuge einer Ausschreibung wird praktisch genügend Zeit für die entsprechenden Vorbereitungen lassen, bei einer Rückholung erscheint dies in vielen Fällen jedoch nicht der Fall. Eventuell könnte eine solche Regelungen dahingehend ausgestaltet werden, dass sowohl für Behörden und Zustelldienste als auch den „neuen" EuZD die Möglichkeit besteht, innerhalb einer bestimmten Frist diesem Eintritt zu widersprechen, und dass eine solche Möglichkeit zB auf der Internetseite des BKA veröffentlicht werden muss (vgl § 30 Abs 3 ZustG). Eine solche Regelung hinsichtlich des automatischen Eintritts würde sich zB als Absatz 3 in § 32 ZustG anbieten. Als Vorbild und zur Erläuterung der Intention einer solchen Regelung würde sich an dieser Stelle exemplarisch § 14 MRG[214] anbieten, der für bestimmte Personen bei Tod des Mieters einen automatischen Eintritt in das Vertragsverhältnis (den Mietvertrag) vorsieht, sofern die berechtigte Person nicht binnen vorgegebener Frist widerspricht. Es versteht sich von selbst, dass sich diese Regelung auf einen gänzlich anderen Rechtsbereich bezieht, jedoch könnte ihre Rechtsfolge als Vorbild für die Lösung der hier diskutierten Problematik dienen. Auch

[214] § 14 Abs 2 MRG lautet: „Nach dem Tod des Hauptmieters einer Wohnung treten in den Mietvertrag mit Ausschluss anderer zur Erbfolge berufenen Personen die im Abs. 3 genannten eintrittsberechtigten Personen ein, sofern sie nicht binnen 14 Tagen nach dem Tod des Hauptmieters dem Vermieter bekannt geben, dass sie das Mietverhältnis nicht fortsetzen wollen. Mit dem Eintritt haften die eintretenden Personen für den Mietzins und die Verbindlichkeiten, die während der Mietzeit des verstorbenen Hauptmieters entstanden sind. […]".

eine entsprechende Haftungsregelung für bereits bestehende Verbindlichkeiten des bisherigen EuZD sollte nicht fehlen.

9.8 Zusammenfassung

Die Lösung mit zwei Auftragsverträgen gem § 1002 ff ABGB erscheint in Summe die praktikabelste, da im Gegensatz zur Inkassozession sämtliche Forderungen zwischen den Parteien personell unverändert bestehen bleiben und sich somit auch an der finanziellen Risikoverteilung nichts ändert. Außerdem scheidet Inkassozession schon deshalb aus, weil es sich dabei um ein Factoringgeschäft handeln würde, welches den Banken vorbehalten ist. Durch die Befugnis des EuZD zur Fälligstellung der Zustellentgelte kann erreicht werden, dass der Verrechnungsablauf zentral koordiniert erfolgt. Dies ergibt sich daraus, dass sich die Verpflichtung zur Mahnung sowie deren Periodizität und die Einhebung und Weiterleitung des Vorschusses gem § 1014 ABGB als Zustellentgelt aus zwei verschiedenen Verträgen ergeben, die vom EuZD koordiniert und abgestimmt werden müssen. Auch die Verrechnung der Verrechnungsleistung basiert bei dieser Konstruktion auf einer vertraglichen Basis, dem entgeltlichen Auftragsvertrag zwischen EuZD und den Behörden (b), und entspricht in der Form daher den Anforderungen des ZustG (§ 29 Abs 2 aE). Wie dargelegt besteht alternativ jedoch auch die Möglichkeit, dass bereits im Zustellrahmenvertrag zwischen Behörde und ZD eine detaillierte Fälligkeitsregelung gem §§ 1417 1. Fall iVm 904 ABGB getroffen wird, sodass es keiner gesonderten Einmahnung mehr bedarf. Wünschenswert wäre jedoch eine gesetzliche Regelung für den Fall, dass der Zustellkopf von einem Betreiber zu einem anderen überführt werden muss. Hier sollte der neue Betreiber hinsichtlich der Ermittlungs- und Verrechnungsleistung automatisch (mit Widerspruchmöglichkeit) in die bestehenden Rechtsverhältnisse eintreten.

10. Die Zustellung ohne Einsatz von Zustelldiensten

Mit dem Verwaltungsverfahrens- und Zustellrechtsänderungsgesetz 2007 wurden weitere Verfahren zur elektronischen Zustellung behördlicher Dokumente in das österreichische Verwaltungsverfahrensrecht aufgenommen, mit welchen praktischen Anforderungen aus dem behördlichen Alltag Rechnung getragen wurde: Die Zustellung an eine elektronische Zustelladresse, die Zustellung über ein Kommunikationssystem einer Behörde und die unmittelbare elektronische Ausfertigung (§§ 37 und 37a ZustG). All diesen Verfahren ist gemeinsam, dass mit ihnen lediglich eine Zustel-

lung ohne Zustellnachweis möglich ist.[215] Möchte eine Behörde selbst elektronisch mit Zustellnachweis zustellen, muss sie dafür entweder einen gem § 30 ZustG zugelassenen Zustelldienst beauftragen oder einen solchen selbst implementieren, der jedoch ebenfalls einer Zulassung bedarf. Eine Unterscheidung zwischen behördlichen und privaten Zustelldiensten sieht das ZustG in seiner aktuellen Fassung nicht mehr vor.[216]

10.1 Die Zustellung an eine elektronische Zustelladresse

§ 37 ZustG regelt im ersten Fall die Zustellung von Dokumenten an eine elektronische Zustelladresse iSd § 2 Z 5 ZustG, worunter „*eine vom Empfänger der Behörde für die Zustellung in einem anhängigen oder gleichzeitig anhängig gemachten Verfahren angegebene elektronische Adresse"* zu verstehen ist. Unter einer solchen elektronischen Adresse ist jede Art einer Adresse zu verstehen, an welcher der Empfänger in elektronischer Form erreichbar ist. Davon umfasst sind E-Mail-Adressen und Fax[217], aber auch Kontaktdaten für Internettelefonie, Instant-Messaging-Dienste[218] oder Postfächer in sozialen Netzwerken. Diese elektronische *Zustell*adresse ist jedoch strikt von einer bekannt gegebenen elektronischen Adresse zu unterscheiden, an welche ein Zustelldienst Benachrichtigungen über das Bereitliegen von zuzustellenden Dokumenten gem § 35 Abs 1 ZustG übermittelt.[219]

Die zweite wichtige Voraussetzung für die Zulässigkeit einer Zustellung an eine solche elektronische Zustelladresse ist, dass diese der Behörde entweder bei Verfahrenseinleitung oder im Zuge eines bereits anhängigen Verfahrens vom Empfänger bekannt gegeben wurde. Diese Adresse muss der Behörde somit aktiv und mit Wissen und Willen des Empfängers bekannt gegeben worden sein, um an diese rechtsverbindlich Zustellungen durchführen zu können. Folglich ist es nicht zulässig, dass die Behörde beispielsweise eine solche Adresse selbst eruiert (zB durch Nachschau auf einer Homepage) oder aus einem anderen, parallel geführten bzw früheren Verfahren verwendet. Dadurch soll sichergestellt werden, dass der Empfänger nach wie vor Zusendungen an dieser Adresse abruft und somit mit hoher Wahrscheinlichkeit von einer Kenntnisnahme ausgegangen werden kann. Eine solche aktive Bekannt-

[215] Vgl Erl zur RV BlgNR 294 23. GP, 2.
[216] Erl zur RV BlgNR 294 23. GP, 3 und 22.
[217] Erl zur RV BlgNR 294 23. GP, 24.
[218] *Larcher*, Zustellrecht, RN 434.
[219] ERL zur RV BlgNR 294 23. GP, 17.

gabe liegt beispielsweise bei deren Angabe im Briefkopf eines Anbringens, bei Anführung in einem Antragsformular oder bei Einbringung eines Anbringens über eine solche elektronische Adresse vor.[220]

Für den Zeitpunkt des Eintritts der Zustellwirkung stellt das Zustellgesetz eine gesetzliche Vermutung auf: Die Zustellung soll zu jenem Zeitpunkt als bewirkt gelten, zu welchem das Dokument beim Empfänger einlangt. Fraglich ist in diesem Zusammenhang jedoch, wann der Tatbestand des „Einlangens“ erfüllt ist: so kann entweder der Eingang im E-Mail-Postfach des Empfängers am Server gemeint sein oder erst der tatsächliche Abruf durch diesen. „Einlangen“ wird in diesem Zusammenhang so zu verstehen sein, dass das Dokument derart in den Verfügungsbereich des Empfängers gebracht wird, dass er von dessen Inhalt Kenntnis nehmen kann. Ratio der gesetzlichen Zustellregelungen ist es, einerseits dem Empfänger die Kenntnisnahme des Inhalts des zuzustellenden Dokuments zu ermöglichen, andererseits muss aber verhindert werden, dass dieser den Eintritt der Zustellwirkung und somit die Auslösung von Rechtsfolgen verhindern kann.[221] Für die physische Zustellung sehen die §§ 26 Abs 1 iVm 17 Abs 2 ZustG den Zustellvorgang als abgeschlossen an, wenn das zuzustellende Dokument in die für die Abgabestelle bestimmte Abgabeeinrichtung (zB Briefkasten, Hausbrieffach, etc) eingelegt wurde.[222] Aus diesem Grund ist davon auszugehen, dass auch bei der Zustellung eines Dokuments an einer elektronischen Zustelladresse gem § 37 ZustG die Zustellwirkung dann eintritt, wenn das Dokument erfolgreich an das E-Mail-Postfach des Empfängers übermittelt wurde. In diesem Fall befindet es sich einerseits derart im Verfügungsbereich des Empfängers, dass dieser vom Inhalt Kenntnis nehmen kann, andererseits kann er den Eintritt der Zustellwirkungen nicht beispielsweise durch Unterlassung des Abrufs der Nachrichten vereiteln. Diese Ansicht entspricht auch der Systematik der Zustellung über ein elektronisches Kommunikationssystem einer Behörde (§ 37 2. Fall ZustG), welche ebenfalls auf die Abrufbarkeit und nicht auf den tatsächlichen Abruf abstellt – mit dem wesentlichen Unterschied, dass hier bis zum Eintritt der Zustellwirkung eine „Toleranzfrist“ bis zum 3. Werktag nach erstmaliger Bereithaltung gewährt wird. Weiters entspricht dies auch der Systematik des Zugangs von elektronischen Willenserklärungen im Bereich des E-Commerce (§ 12 ECG), wo deren Bindungswirkung eben-

[220] Vgl ERL zur RV BlgNR 294 23. GP, 17.
[221] Vgl *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 353.
[222] Die Zustellwirkung tritt hier gem § 26 Abs 2 ZustG jedoch erst am 3. Werktag nach Übergabe ein. jedoch

falls bereits zum Zeitpunkt des Zugangs im E-Mail-Postfach eintritt.[223] Jedoch gelten Willenserklärungen, welche in den Nachtstunden oder am Wochenende einlangen, erst am Morgen des folgenden Werktags als zugegangen, da erst dann „unter gewöhnlichen Umständen“ mit deren Abruf und somit ihrer Kenntnisnahme gerechnet werden kann. Dass dies auch für eine Zustellung an eine elektronische Zustelladresse gem § 37 1. Fall ZustG der Fall ist, erscheint aber zweifelhaft, da § 37 ZustG dezidiert auf den Zeitpunkt des Einlangens im Verfügungsbereich des Empfängers und nicht auf die Möglichkeit des Abrufs unter gewöhnlichen Umständen abstellt.

Im Zweifel ist der Zeitpunkt des tatsächlichen Einlangens von der Behörde zu beweisen, wodurch allein auf Grund der Behauptung des Empfängers, dass eine Zustellung nicht oder nicht zu diesem Zeitpunkt erfolgt sei, diese gesetzliche Vermutung gegenstandslos wird. Treten beim Zustellvorgang technische Probleme auf, so ist dies nach der Sphärentheorie zu lösen: Liegen die technischen Schwierigkeiten im Machtbereich des Empfängers (Hard- oder Softwareprobleme), so war die Zustellung erfolgreich. Störungen am Übertragungsweg hingegen gehen zu Lasten der Behörde und die Zustellung gilt als nicht bewirkt.[224] Fraglich ist in diesem Zusammenhang nun weiters, welche Datenformate (insb proprietäre) für eine erfolgreiche Zustellung von der Behörde verwendet werden dürfen, da nicht davon ausgegangen werden kann, dass jeder Empfänger über dieselben Softwareprodukte (und darüber hinaus auch in einer kompatiblen Version[225]) wie die Behörde verfügt. Von einer erfolgreichen Zustellung wird man mMn dann ausgehen dürfen, wenn die Behörde ein Datenformat verwendet, welches als Standardformat iSd § 21 Abs 2 E-GovG zu qualifizieren ist. Dies wird aktuell jedenfalls PDF(/A), HTML und reiner (Plain-)Text sein, höchstwahrscheinlich aber auch die entsprechenden Dateiformate von Open Office[226], Libre Office[227] und Microsoft Office[228].

[223] Vgl *Zankl*, Rechtsqualität und Zugang von Erklärungen im Internet, ecolex 2001, 344, mwN.
[224] Vgl *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, 387.
[225] Beispielsweise kann ein Dokument im Microsoft Word 2007-Format (*.docx) mit Microsoft Word 2003 nur bei vorheriger Installation eines Kompatibilitäspaketes verarbeitet werden.
[226] www.openoffice.org.
[227] http://www.libreoffice.org.
[228] Eine Aufzählung aller möglichen Dateiformate muss an dieser Stelle unterbleiben, jedoch sei zB auch an Bild-, Musik- und Videodateien gedacht.

10.2 Die Zustellung über ein Kommunikationssystem

Für Zustellungen ohne Zustellnachweis sieht § 37 ZustG weiters vor, dass die Behörde selbst ein Kommunikationssystem betreiben kann, über welches Empfänger ihre zuzustellenden Dokumente abrufen können. Die Zustellwirkung tritt in einem solchen Fall am dritten Tag nach erstmaligem Bereithalten des Dokuments im Kommunikationssystem ein. Wie die technische Implementierung eines solchen Systems zu erfolgen hat, wird im Gegensatz zu den zugelassenen Zustelldiensten nicht weiter konkretisiert, jedoch müssen die Datensicherheitsmaßnahmen gem § 14 DSG entsprechend umgesetzt werden. Dies umfasst jedenfalls die Implementierung eines entsprechenden Zugangsberechtigungssystems, um unberechtigte Zugriffe auf Dokumente und somit personenbezogene Daten zu verhindern. Es darf nur dem entsprechenden Empfänger möglich sein, auf seine Zustellstücke zuzugreifen. Ein solches Zugangsberechtigungssystem muss derart ausgestaltet sein, dass die *eindeutige* Identität (§ 2 Z 2 E-GovG) der zugreifenden Person festgestellt und die Authentizität nachgewiesen werden kann (§ 3 Abs 1 E-GovG). Die Zustellung über ein solches Zustellsystem der Behörde muss jedoch dann unterbleiben, wenn der Empfänger bei einem zugelassenen elektronischen Zustelldienst angemeldet ist (§ 37 Abs 2 ZustG). Dies hat die Behörde somit durch vorherige Abfrage beim Zustellkopf zu prüfen, bevor sie eine Zustellung über ihr eigenes Zustellsystem verfügen darf.

Der entscheidende Nachteil dieser Variante ist offensichtlich, nämlich dass der Bürger für jedes dieser Systeme eigene Zugangsdaten verwalten muss und in all diesen Systemen ggf auch die Daten zu seiner Person aktuell halten muss. Mit der Schaffung behördenübergreifender zugelassener elektronischer Zustelldienste wollte man diesem Umstand begegnen, in dem solche Zustelldienste sozusagen als „Single Point of Contact“ die einzige Kommunikationsschnittstelle zwischen Bürgern und Behörden bilden (sollten).[229] Dieser zentrale Kommunikationspunkt soll als Ersatz für eine Vielzahl einzelbehördlicher Lösungen dienen, wofür die Regelung des § 37 Abs 2 ZustG offenbar unterstützend wirken soll.[230]

[229] *Larcher*, Zustellrecht, RZ 472, mwN.
[230] Vgl Erl zur RV 294 BlgNr 23. GP, 25.

Der aktuell wohl bekannteste Vertreter eines solchen Kommunikationssystems ist FinanzOnline[231] des BMF[232]. Detaillierte Regelungen dazu finden sich in der FinanzOnline-Verordnung 2006 (FOnV 2006[233])[234]. Zu beachten ist jedoch auch, dass der gesamte 3. Abschnitt des ZustG nicht für Zustellungen in Finanzangelegenheiten anzuwenden ist (§ 98 BAO)[235].

10.3 Unmittelbare elektronische Ausfolgung

Gemäß § 37a ZustG kann die Zustellung auch durch unmittelbare Ausfolgung erfolgen, wenn Antragstellung und Zustellung in einem sehr engen zeitlichen Zusammenhang stehen und in derselben technischen Umgebung erfolgen (zB unter Verwendung einer Webapplikation im Zuge ein und derselben Sitzung „Online-Dialogverkehr“). Ist auch ein Zustellnachweis erforderlich, ist dieser unter Einsatz der Bürgerkarte zu erbringen.[236]

11. Die Erbringung weiterer Leistungen im Auftrag Privater

Die Leistungen der Zustelldienste bieten nicht nur für Behörden die Möglichkeit einer qualitätsvollen und nachvollziehbaren Übermittlung von Dokumenten, sondern können darüber hinaus auch für die Privatwirtschaft wertvolle Dienste leisten. Auch im nicht hoheitlichen Bereich gibt es eine Reihe von Situationen, in welchen der Zugang bestimmter Dokumente beim Empfänger nachweislich erfolgen soll, sodass dieser den Erhalt nicht bestreiten kann. Weiters garantiert die qualitätsvolle Übermittlung auch eine entsprechende Vertraulichkeit, Authentizität und Integrität des Inhalts. § 29 Abs 3 1. Satz ZustG eröffnet den Zustelldiensten die Möglichkeit, neben der hoheitlichen Zustellleistung auch weitere beliebige Leistungen auf privatrechtlicher Basis erbringen zu können. Die Bandbreite an solchen Leistungen wird dabei nicht beschränkt, sodass auf diese Weise beliebig weitere Leistungen angeboten werden können. Insbesondere die nachweisliche Zusendung von Dokumenten im Auftrag Privater wird vom Gesetz ausdrücklich genannt.

---

[231] https://finanzonline.bmf.gv.at.
[232] Vgl Erl zur RV 294 BlgNr 23. GP, 25.
[233] BGBl II 97/2006 idF BGBl II Nr 82/2011.
[234] Vgl *Larcher*, Zustellrecht, RN 437 ff.
[235] Die Zustellwirkung tritt bei Finanz Online analog zum Bereich des Zivilrechts (vgl § 12 ECG) bereits unmittelbar mit Bereithaltung in der DataBox ein (§ 98 Abs 2 BAO).
[236] Vgl Erl zur RV BlgNR 294 23. GP, 24.

11.1 Die Ermittlungsleistung im Auftrag Privater

Damit der Zustellkopf als zentrales Verzeichnis aller bei einem Zustelldienst angemeldeten Empfänger auch für die privatrechtliche elektronische Übermittlung von Dokumenten verwendet werden kann, sieht § 29 Abs 3 2. Satz ZustG vor, dass die Ermittlungsleistung (nicht aber die Verrechnungsleistung!) auch für die Zusendung von Dokumenten im Auftrag von Privaten in derselben Form in Anspruch genommen werden kann wie für hoheitliche Zustellungen. Zu denselben Bedingungen bedeutet, dass auch für eine privatwirtschaftliche Zusendung ausschließlich die Suchkriterien gem § 34 Abs 2 lS ZustG für eine Abfrage beim Zustellkopf verwendet und lediglich die Angaben des § 34 2. Satz ZustG in der Antwort beinhaltet sein dürfen.[237] Dies stellt auch den datenschutzrechtlichen gesetzlichen Erlaubnistatbestand zur Übermittlung personenbezogener Daten dar (§§ 7 Abs 2 iVm 8 Abs 1 Z 1 DSG). Als Suchkriterien sind im Zuge einer Privatzusendung somit Name bzw Bezeichnung des Kunden, ggf Geburtsdatum bei natürlichen Personen, wbPK bzw SZ, elektronische Verständigungsadresse und physische Verständigungsadresse zulässig (§ 33 Abs 1 Z 1 – 5 ZustG).[238] Problematisch in diesem Zusammenhang erscheint jedoch, dass § 33 Abs 1 Z 3 lit a ZustG lediglich auf das bPK gem § 9 E-GovG verweist, welches dem Anfragenden im Fall der Privatzusendung jedoch nicht vorliegt bzw vorliegen darf, sondern lediglich das wbPK gem §§ 14 f E-GovG. Hierbei dürfte es sich aller Wahrscheinlichkeit nach um eine planwidrige Lücke handeln, da sich § 34 Abs 2 2. Satz ZustG gleichermaßen auf die behördliche Zustellung und privatrechtliche Zusendung bezieht (vgl Satz 1).

Die Antwort des Zustellkopfs darf ausschließlich die Internetadresse jenes oder jener Zustelldienste(s), bei welchen der Kunde angemeldet ist, die akzeptierten Dateiformate und Angaben zur inhaltlichen Verschlüsselung (§ 33 Abs 1 Z 6 u 7 ZustG) beinhalten.[239] Anders als bei einer behördlichen Zustellung wird der Verrechnungstoken jedoch technisch etwas anders generiert und dabei anstatt des bPK das wbPK des Empfängers verwendet (vgl ZUSEPRIV[240]). Da der Verrechnungstoken jedoch

[237] RV 294 BlgNr 23. GP, 21.
[238] Dies ergibt sich aus der eindeutigen Verweiskette des ZustG: §§ 29 Abs 3 2. Satz iVm Abs 2 Z 2 iVm 34 Abs 1 1. und 2. Satz iVm 33 Abs 1 Z 6 und 7 und Abs 2 sowie § 34 Abs 2 2. Satz, der auf die behördliche Zustellung als auch die privatrechtliche Zusendung gleichermaßen verweist.
[239] RV 294 BlgNr 23. GP, 21.
[240] *Tauber/Rössler/Reichstädter*, Nachweisliche Zusendung im Auftrag von Privaten, 14.

nur verschlüsselt an den Abfragenden übermittelt wird, bedarf es keiner gesetzlichen Ermächtigung zur Datenübermittlung, da sich deren Zulässigkeit bereits daraus ergibt, dass die im Token beinhalteten personenbezogenen Daten lediglich indirekt personenbezogen (also verschlüsselt) übermittelt werden (§§ 7 Abs 2 iVm 8 Abs 2 2. Fall DSG).

11.2 Das Rechtsverhältnis bei der Erbringung weiterer Leistungen

Vereinbart ein Zustelldienst mit seinen Kunden neben der Erbringung von Zustellleistungen auch die Erbringung bestimmter sonstiger Leistungen, so handelt es sich hierbei zweifellos um den Abschluss eines zivilrechtlichen Vertrags zwischen Kunde und Zustelldienst über die jeweilig zu erbringende(n) Leistung(en). Solche (zusätzlichen) Leistungen werden im Unterschied zur Erbringung der Zustellleistung gem § 29 Abs 1 Z 1 – 9 ZustG jedoch gänzlich und ausschließlich im Interesse des Kunden (und nicht im Auftrag der Behörde) erbracht[241], wodurch auch das Rechtsverhältnis bestehend aus Leistung und Gegenleistung ausschließlich zwischen diesen beiden Parteien begründet wird. Die Pflicht des Zustelldienstes zur Erbringung einer solchen Leistung ergibt sich somit ausschließlich aus dem Vertrag zwischen Zustelldienst und Kunde, da eine solche Leistung allein der Gegenleistung wegen (dem zu entrichtenden Entgelt) erbracht wird. Es handelt sich dabei somit um einen vollkommen zweiseitigen Vertrag.[242] Um welchen konkreten Vertragstyp es sich bei der Erbringung einzelner weiterer Leistungen handelt, ist im Einzelfall und abhängig von der Art der Leistung zu beurteilen. Der Zustelldienst ist hier – im Gegensatz zur Erbringung der Zustellleistung – jedoch nicht an bestimmte gesetzliche Preisvorgaben gebunden (vgl § 29 Abs 1 aE ZustG) und kann die Preise für seine Leistungen frei festsetzen. Auch besteht für die Erbringung solcher Leistungen keine Zulassungspflicht (§ 4 ECG).

11.3 Mögliche weitere Leistungen eines Zustelldienstes

Es besteht keine Einschränkung, welche weiteren Leistungen ein Zustelldienst anbieten und erbringen kann, wodurch dieser in der Gestaltung seines Leistungsangebots frei ist. Lediglich die allgemeinen rechtlichen Rahmenbedingungen sind – wie bei der Ausübung jeder wirtschaftlichen Tätigkeit – zu berücksichtigen.

---

[241] Vgl *Raschauer/Sander/Wessely*, Österreichisches Zustellrecht, 191; *Feil*, Zustellwesen, 87.
[242] Vgl *Koziol/Welser/Kletecka*, Bürgerliches Recht I, 115.

Weitere denkbare privatrechtliche Leistungen, die bereits vom ZustG vorgezeichnet werden, sind die dauerhafte qualitätsvolle Speicherung von Dokumenten („Dokumentensafe“) gem § 35 Abs 4 IS ZustG, die physische Übermittlung eines Datenträgers mit den elektronischen Dokumenten bzw die Zusendung von Ausdrucken solcher (§ 29 Abs 1 Z 10 ZustG) und die Weiterleitung von Dokumenten an den ERV (§ 29 Abs 1 Z 11 ZustG).

11.3.1 Die dauerhafte Speicherung von Dokumenten

Eine heutzutage bereits sehr weit verbreitete Leistung ist die (qualitätsvolle) internetbasierte Speicherung von Dokumenten in Form von Cloud Computing Services. Eine solche Speicherleistung ist jedoch unabhängig von der Bereithaltung (und somit Speicherung) im Zuge der Erbringung der Zustellleistung zu beurteilen, da diese in diesem Kontext nicht mehr als Teilleistung der Zustellleistung iSd § 29 Abs 1 Z 5 ZustG zu qualifizieren ist. Diese beiden Leistungen – also die Bereithaltung zur Abholung im Zuge der Zustellleistung und die Speicherung von Dokumenten im Auftrag Privater – erfüllen aus datenschutzrechtlicher Sicht auch verschiedene Zwecke, da im ersten Fall der Zweck der Verarbeitung die Übermittlung der zuzustellenden Dokumente in die Sphäre des Empfängers im Auftrag der Behörde ist, im zweiten Fall eben lediglich die Bereitstellung von Online-Speicherplatz. Aus diesem Grund muss auch für jeden dieser beiden Fälle separat ein Erlaubnistatbestand für die Zulässigkeit der Verarbeitung der jeweils zu speichernden Daten gem der §§ 8 oder 9 DSG erfüllt sein (§ 7 Abs 1 DSG). Im ersten Fall bildet diesen eine gesetzliche Grundlage (§ 29 Abs 1 Z 5 ZustG) und im zweiten Fall die vertragliche Vereinbarung zwischen Kunden und Zustelldienst (§ 8 Abs 1 Z 4 iVm Abs 3 Z 4 DSG), wobei nahe liegender Weise aber auch das Einverständnis des Kunden angenommen werden kann (§ 8 Abs 1 Z 2 DSG). Da die Datenspeicherung als weitere Leistung wohl auch ein anderes Aufgabengebiet des Zustelldienstes darstellen wird und die „Übernahme“ von Daten aus dem Aufgabengebiet der Erbringung hoheitlicher Zustellleistungen eine Datenübermittlung iSd § 4 Z 12 DSG darstellen wird, ist auch hierfür gem § 7 Abs 2 DSG ein datenschutzrechtlicher Erlaubnistatbestand zu erfüllen. Ein solcher findet sich wiederum im Gesetz (§ 35 Abs 4 aE ZustG), in der zivilrechtlichen Vereinbarung zwischen Kunde und Zustelldienst oder in der Einwilligung des Kunden.

11.3.2 Erstellung und Übermittlung von Ausdrucken oder Datenträgern

Bei der Erbringung dieser Leistung ist mMn davon auszugehen, dass diese ebenfalls aufgrund einer vertraglichen Basis zwischen Zustelldienst und Empfänger zu erbringen ist. Dies begründet sich damit, dass die Zustellwirkung auch ohne die Inanspruchnahme dieser Leistung eintritt und diese Leistung somit nicht mehr als Teil der Zustellleistung im engeren Sinn angesehen werden kann[243]. Sie dient lediglich dazu sicherzustellen, dass der Empfänger auch dann Kenntnis vom Inhalt der zugestellten Dokumente erlangen kann, wenn dieser Probleme mit dem Abruf oder der Lesbarkeit (zB auf Grund von Softwareinkompatibilitäten) haben sollte. Die Zustellwirkung tritt ja bereits mit Abholung der Dokumente (also mit dem Login) ein, unabhängig davon, ob diese im Anschluss gespeichert oder geöffnet werden können. Weiters hat auch nicht mehr die Behörde, in deren Auftrag die Dokumente zugestellt wurden, die für diese Leistung entstehenden Kosten als Gegenleistung zu tragen, sondern der Empfänger (§ 29 Abs 1 lS ZustG). Dies legt den Schluss nahe, dass bezüglich dieser Leistung eine vertragliche Verbindung zwischen Zustelldienst und Empfänger notwendig ist, da auch in diesem Verhältnis das Synallagma zu finden ist. Der Zustelldienst erbringt diese Leistung ja nicht mehr des Entgelts für die Zustellleistung wegen, sondern des Entgelts für die Erbringung dieser Zusatzleistung wegen, da letztere nicht im Entgelt für die Zustellleistung inbegriffen ist. Bezüglich dieser Leistung besteht das Synallagma somit zwischen Empfänger und Zustelldienst.

Nichtsdestotrotz muss diese Leistung vom Zustelldienst verpflichtend angeboten werden, um eine Zulassung als Zustelldienst zu erhalten, da es sich bei dieser Liste an Leistungen um Mindestleistungen handelt[244]. Aus praktischen Gründen kann dies jedoch dann nicht der Fall sein, wenn das Dokument ausschließlich verschlüsselt vorliegt, da dem Zustelldienst eine Entschlüsselung nicht möglich ist.[245] Daraus und aus dem Terminus „auf dessen Verlangen“ in § 29 Abs 1 Z 10 aE ZustG wird man folglich schließen können, dass der Zustelldienst in Bezug auf die Erbringung dieser Leistung ebenfalls einem (gesetzlich angeordneten) Kontrahierungszwang unterliegt und der Kunde somit einen durchsetzbaren Anspruch auf deren Erbringung (zu den

[243] Vgl *Raschauer/Sander/Wessely*, Österreichisches Zustellrecht, 191; *Feil*, Zustellwesen, 87; Erl zur RV BlgNR 294 23. GP, 21.
[244] Erl zur RV BlgNR 252 22. GP, 16.
[245] Erl zur RV BlgNR 294 23. GP, 21.

üblichen Bedingungen) hat (vgl Kapitel 3.3.4). Auch die monopolartige Stellung[246] des Zustelldienstes kann bezüglich dieser Leistung bejaht werden, da auch nur dieser über die zu übermittelnden Dokumente verfügt.

11.3.3 Die Weiterleitung zugestellter Dokumente an den ERV

Mit dem Budgetbegleitgesetz 2011 (BGBl I 111/2010), das mit 1. 1. 2011 in Kraft trat, wurde mit Z 11 in § 29 Abs 1 ZustG eine weitere Leistung eingeführt. Diese Leistung umfasst „*die Weiterleitung eines zuzustellenden Dokuments zur elektronischen Übermittlung nach den §§ 89a ff GOG auf Verlangen des Empfängers sowie die Mitteilung an die Behörde, wann das zuzustellende Dokument in den elektronischen Verfügungsbereich des Empfängers (§ 89d GOG) gelangt ist*“, sofern der Zustelldienst diese Leistung anbietet. Der Kunde soll wählen können, ob ein einzelnes konkretes Dokument, eine bestimmte Art von Dokumenten auf Grund genereller Merkmale oder alle Dokumente an den ERV weitergeleitet werden.[247] Die Zustellung und somit der Eintritt der Zustellwirkung soll demnach entsprechend der Regelungen des GOG erfolgen (§ 35 Abs 9 ZustG). Dies stellt hinsichtlich der Weiterleitung von Zustellstücken nach bestimmten Kriterien oder aller Zustellstücke kein Problem dar, da diese automatisiert weitergeleitet werden können. Wie jedoch der Fall einer individuellen Weiterleitung eines Zustellstücks rechtlich zu beurteilen ist, ist fraglich. Gemäß den EB soll sich der Zeitpunkt der Zustellung nach § 89d Abs 2 GOG richten.[248] Der Empfänger muss die Weiterleitung individueller Zustellstücke jedoch auch individuell (zB durch Klick auf einen Button) veranlassen, wofür aber ein Login beim Zustelldienst notwendig ist. Somit tritt die Zustellwirkung gem § 35 Abs 5 ZustG aber bereits auf Grund der digitalen Signatur bei der Anmeldung beim Zustelldienst ein und die Zustellung ist bereits zu diesem Zeitpunkt entsprechend der Regelungen des ZustG abgeschlossen. Ein weiterer Eintritt der Zustellwirkung gem §§ 89a ff GOG ist somit nicht möglich, wodurch die individuelle Weiterleitung von Dokumenten an den ERV folglich keine rechtliche Wirkung mehr entfalten wird können, da jede weitere Zustellung ein und desselben Zustellstücks keine rechtliche Wirkung hat (§ 6 ZustG). Auch bei den anderen beiden Varianten wird es gem § 6 ZustG wohl darauf ankommen, in welchem (technischen) System – also Zustelldienst oder ERV – der Empfänger die Zustellstücke zuerst abruft. Ungeklärt ist in diesem Zusammenhang auch, wie der

[246] Vgl *Zankl*, Bürgerliches Recht, RZ 52.
[247] Vgl Erl zur RV BlgNR 981 24. GP, 44.
[248] Erl zur RV BlgNR 981 24. GP, 44.

Begriff „Weiterleitung“ technisch zu interpretieren ist, also ob der Zustelldienst das Zustellstück weiter bereithalten muss oder ob er dieses nach erfolgreicher Weiterleitung an den ERV löschen darf bzw muss.

Aufgrund des Terminus „*sofern der Zustelldienst diese Leistung anbietet*“ in Z 11 zeigt sich sehr offensichtlich, dass diese Leistung im Gegensatz zu jener der Z 10 offenbar nicht notwendigerweise für eine Zulassung als Zustelldienst angeboten werden muss. Fraglich ist jedoch, ob bezüglich dieser Leistung analog zu jener der Z 10 das Bestehen eines Kontrahierungszwangs angenommen werden muss. Dies wird konsequenterweise wohl zu bejahen sein, jedoch ist der Zustelldienst nicht gezwungen, eine solche Leistung überhaupt anzubieten. Bietet er sie an, so wird jedermann einen durchsetzbaren Anspruch auf Abschluss eines dementsprechenden Vertrags haben.

Weiters geht aus dem ZustG – im Gegensatz zu allen anderen aufgezählten Leistungen – nicht hervor, wer das Entgelt für diese Leistung zu erbringen hat. Eine entsprechende Regelung dürfte im Zuge der Novelle wohl übersehen worden sein. Der Behörde werden die Kosten für diese Leistung wohl nicht aufgebürdet werden können, da deren Rechtsgrund signifikant höher der Sphäre des Kunden zuzurechnen ist. Analog zu Z 10 ist somit auch in diesem Fall das Synallagma zwischen Empfänger und Zustelldienst zu finden, da es ausschließlich auf die Willenserklärung des Empfängers ankommt (zB Klick auf einen Button oder Einstellung entsprechender Filter), ob diese Leistung vom Zustelldienst ausgeführt werden muss oder nicht. Die Pflicht zur Leistung des Entgelts wird somit auch den Empfänger treffen müssen.

11.4 Der Zustelldienst als Diensteanbieter im Sinn des ECG

In diesem Zusammenhang ist nun zu prüfen, ob es sich bei den Zustelldiensten um Diensteanbieter iSd ECG handelt, worunter § 3 ECG „*eine natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die einen Dienst der Informationsgesellschaft bereitstellt“* versteht. Als Dienst der Informationsgesellschaft definiert das ECG solche Dienste, die

- in der Regel gegen Entgelt
- elektronisch

- im Fernabsatz
- auf individuellen Abruf des Empfängers

bereitgestellt werden.

Betrachtet man nun die Leistungen der Zustelldienste, so zeigt sich, dass alle dieser vier Voraussetzungen erfüllt sind: Dass solche Leistungen elektronisch und im Fernabsatz – also bei nicht gleichzeitiger physischer Anwesenheit der Vertragspartner – bereitgestellt werden, ist offensichtlich, da die Leistungen idR über das Internet bereitgestellt und in den meisten Fällen auch gleich elektronisch erbracht werden. Weiters werden sämtliche Leistungen von Zustelldiensten auch nur auf individuelle Veranlassung durch den Kunden und individuell für diese erbracht, wodurch jeder Kunde in der Lage ist, den Inhalt des Dienstes gesondert und für sich individualisiert in Anspruch zu nehmen. Die Erbringung solcher Dienste erfolgt seitens der Zustelldienste stets entgeltlich, auch wenn der Kunde für manche Leistungen (wie beispielsweise den Empfang und den Abruf von Dokumenten im Auftrag von Privaten) unmittelbar kein Entgelt zu entrichten hat. Dennoch handelt der Zustelldienst in einem entgeltlichen Rahmen und mit Ertragsabsicht, auch wenn Leistungen vereinzelt unentgeltlich erbracht werden.[249] Dass die Inanspruchnahme solcher Dienste nicht nur über für den Menschen leicht bedienbare Benutzeroberflächen (User Interfaces) sondern auch über rein automatisiert ansprechbare Schnittstellen (wie zB Webservices) erfolgen kann, kann an der Anwendbarkeit des ECG nichts ändern. Auch die weiteren Regelungen des ECG sind somit für die Erbringung solcher Leistungen relevant (zB Informationspflichten, Zugang von Willenserklärungen oder die Haftungsprivilegien). Dasselbe gilt auch im Verhältnis zwischen Behörde und Zustelldienst bei der Erbringung der (hoheitlichen) Zustellleistung, da auch hier der Zustelldienst als Verwaltungshelfer der Behörde auf Grund eines mit dieser online abgeschlossenen (und online zu erfüllenden) zivilrechtlichen Vertrags tätig wird. Die einzige Besonderheit ist, dass Zustelldienste im behördlichen Kontext nicht die Zulassungsfreiheit gem § 4 ECG für sich in Anspruch nehmen können, da für solche Fälle dem ZustG als lex specialis Vorrang gebührt.

[249] Vgl *Laga/Sehrschön/Ciresa*, E-Commerce Gesetz, 9 ff.

12. Die Amtssignatur

Wesentliche Voraussetzung für die rechtsverbindliche Durchführung einer elektronischen Zustellung ist, dass die zuzustellenden elektronischen Dokumente mit einer Amtssignatur versehen wurden. § 18 Abs 4 AVG normiert die Formerfordernisse an schriftliche Ausfertigungen: Diese müssen die Bezeichnung der Behörde, das Datum der Genehmigung sowie den Namen des Genehmigenden beinhalten. Weiters muss eine elektronische Ausfertigung an Stelle der händischen Unterschrift mit einer Amtssignatur gem § 19 E-GovG versehen werden. Wird eine elektronische Ausfertigung durch den Genehmigungsberechtigten bereits bei der Genehmigung gem § 18 Abs 3 AVG mit einer Amtssignatur versehen, so erfüllt dies zeitgleich auch die Anforderungen an die Unterschrift für die Ausfertigung gem Abs 4. Eine weitere Unterschrift oder Beglaubigung durch die Kanzlei ist nicht mehr notwendig. Im Anschluss daran kann unmittelbar die elektronische Zustellung der Ausfertigung verfügt werden. Aber auch Ausdrucke amtssignierter Ausfertigungen bedürfen keiner weiteren Unterschrift oder Beglaubigung und sind in der Form rechtsverbindlich.[250]

12.1 Wesen und Rechtswirkungen der Amtssignatur

Die Amtssignatur bildet das Pendant zur Unterschrift und den Amtsstempel bei herkömmlichen Papierausfertigungen und hat sowohl eindeutige Identifizierungsfunktion bezüglich der ausstellenden Behörde (§ 2 Z 2 E-GovG) als auch Authentizitätsfunktion (§ 2 Z 5 E-GovG) für den Inhalt des amtssignierten Dokuments. Die Amtssignatur dient durch verpflichtende Aufbringung der „Bildmarke“ auf das Dokument dazu, die Herkunft des Dokuments von einem Auftraggeber des öffentlichen Rechts für den Empfänger leichter erkennbar zu gestalten. Die Bildmarke ist idR durch das Wappen/Logo und die Bezeichnung des Rechtsträgers charakterisiert.[251] Mit dieser Regelung wurde der Befürchtung begegnet, dass sich aus der Verwendung elektronischer Dokumente eine verminderte Erkennbarkeit des öffentlichen Charakters solcher Ausfertigungen ergeben könnte.[252] Die Bildmarke muss von der Behörde *gesichert*[253] im

[250] Erl zur RV 294 BlgNR 23. GP, 14.

[251] Ein Beispiel einer Bildmarke findet sich auf der Homepage *Digitales:Österreich* unter http://www.austria.gv.at/site/5318/default.aspx (abgerufen am: 17. 1. 2012).

[252] Erl zur RV 252 BlgNR 22. GP, 10.

[253] Als gesicherte Veröffentlichung gelten beispielsweise folgende Lösungen: Die Bildmarke wird einschließlich der Erklärung, dass es sich dabei eben um die Bildmarke der Behörde handelt, in einem seinerseits amtssignierten PDF-Dokument auf der Behördenhomepage einfach auffindbar veröffentlicht. Die zweite Möglichkeit ist die

Internet veröffentlicht werden. Weiters ist im Dokument der Vermerk anzuführen, dass dieses Dokument mit einer Amtssignatur versehen wurde (§ 19 Abs 2 E-GovG).

12.2 Aufbringung der Amtssignatur

§ 19 Abs 1 E-GovG sieht als weiteres Formerfordernis für die Amtssignatur die Aufbringung mindestens einer fortgeschrittenen elektronischen Signatur gem § 2 Z 3 SigG vor, jedoch kann auch eine qualifizierte Signatur nach Ziffer 3a verwendet werden.[254] Weiters muss die Besonderheit der Amtssignatur durch ein entsprechendes Attribut im Signaturzertifikat ausgewiesen werden, was durch die Aufnahme der Verwaltungseigenschaft als X.509-Zertifikateserweiterung (Object Identifier der Verwaltung) erreicht wird.[255]

Da für die Amtssignatur nicht notwendigerweise eine qualifizierte Signatur, für welche das Zertifikat stets auf eine natürliche Person ausgestellt sein muss, zum Einsatz kommen muss, ist die Ausstellung eines einzigen behördenweit einsetzbaren Zertifikats ausreichend. Da auch der Einsatz einer sicheren Signaturerstellungseinheit nicht notwendig ist, kann es sich bei diesem Zertifikat um ein Softwarezertifikat[256] handeln, welches auf einem zentralen Signaturserver installiert wird und der im Anschluss für die gesamte Behörde das Amtssignaturservice zur Verfügung stellt. Nichtsdestotrotz muss darauf geachtet werden, dass dieses Service nicht behördenweit frei verfügbar und beliebig genutzt werden kann, sondern dass dieses nur solchen Personen zugänglich ist, denen auch eine entsprechende Genehmigungsbefugnis zukommt. Da mit der Aufbringung der Amtssignatur sowohl der Genehmigungs- als auch Ausfertigungsprozess gem § 18 Abs 3 und 4 AVG abgeschlossen ist, muss jede Person, die dieses Service nutzt, identifiziert (§ 2 Z 1 E-GovG)[257] und die Authentizität (§ 2 Z 5 E-GovG) der Genehmigung feststellbar sein[258]. Daher muss das Amtssignaturservice technisch so ausgestaltet sein, dass dieses nur von berech-

---

Veröffentlichung der Bildmarke über eine HTTP**S**-Verbindung, wodurch das auf die Behörde ausgestellte Server-Zertifikat geprüft werden kann (*Projektgruppe "Amtssignatur"*, Amtssignatur 2008 – Best practises, 9).

[254] Erl zur RV 290 BlgNR 23. GP, 5.

[255] *Karlinger*, Allgemeine Richtlinien für Amtssignaturzertifikate in der Verwaltung, 3 f.

[256] Beispielsweise in Form einer PKCS#12-Datei.

[257] Eine eindeutige Identifikation gem § 2 Z 2 E-GovG ist in diesem Zusammenhang nicht notwendig, da die Anzahl der Bediensteten zwar abhängig von der Art der Behörde aber dennoch eine mehr oder weniger überschaubare Größe darstellt und somit eine Identifikation der individuellen Person auch nur mit Vor- und Nachname (ggf auch Abteilung oder Ressort) mit sehr hoher Wahrscheinlichkeit möglich ist.

[258] § 18 Abs 3 AVG.

tigten Personen verwendet werden kann. Diese Funktionalität eines Berechtigungssystems kann beispielsweise von einem ELAK-System abgebildet werden.

Die Notwendigkeit der Installation eines Berechtigungssystems ergibt sich auch aus Litera c des § 2 Z 3 SigG, die nicht nur in der Form auszulegen sein wird, dass die Signaturerstellungsdaten unberechtigten Dritten (Außenstehenden) nicht zur Kenntnis gelangen dürfen, sondern die Behörde als Signator auch intern die Kontrolle darüber haben muss, welche konkreten Personen nun die Aufbringung von Amtssignaturen veranlassen können und welche dies im Endeffekt auch getan haben. Da bei der serverbasierten Aufbringung von Amtssignaturen alleine aus der Signatur nicht mehr nachvollziehbar ist, welche konkrete Person den Signaturvorgang ausgelöst hat, muss das genannte Berechtigungssystem auch über eine umfassende Protokollierungsfunktion verfügen, sodass die Nutzung des Amtssignaturservices nachvollziehbar und ggf rückverfolgbar bleibt.

12.3 Die Prüfung der Amtssignatur

Zwar ergibt sich aus § 19 E-GovG nicht explizit die Pflicht zur Bereitstellung einer technischen Möglichkeit, mit welcher die Signatur amtssignierter elektronischer Dokumente geprüft werden kann, jedoch wird man dies implizit wohl annehmen müssen. Anderenfalls wäre die Verpflichtung der Behörde bezüglich der Angabe allgemein verständlicher Informationen, wie die elektronische Signatur geprüft werden kann, obsolet. Aus dieser Gestaltung der Rechtsnorm ist jedoch nicht zwangsläufig zu schließen, dass dieses Signaturprüfservice von der Behörde selbst bereitgestellt werden müsste. So erfüllt ein einfacher Verweis auf ein öffentlich verfügbares Signaturprüfservice – wie beispielsweise jenes der RTR (www.signaturpruefung.gv.at) – diese gesetzliche Anforderung. Existiert jedoch kein allgemein verfügbares Prüfservice, so wird die Behörde aber sehr wohl verpflichtet sein, ein solches zur Verfügung zu stellen.

Für Ausdrucke amtssignierter Dokumente ergibt sich aus § 20 E-GovG die Verpflichtung, dass der Ausdruck entweder durch Rückführung in das elektronische Original[259] prüfbar sein muss oder durch anderweitige Vorkehrungen der Behörde verifi-

[259] In diesem Fall kommt nur eine textuelle Signatur in Frage, bei welcher der (normalisierte) Text aus dem Dokument extrahiert und signiert wird, nicht jedoch andere Elemente wie zB Grafiken.

zierbar sein muss (zB gesicherter Zugang zu einem Bescheidarchiv, Hotline, persönliche Vorlage bei der Behörde, etc)[260]. Zur Rückführung und Prüfung ist der gesamte zu prüfende Text (exklusive Grafiken und anderer Objekte) einschließlich der Daten des Signaturblocks in ein Webinterface einzugeben, welches anschließend die Prüfung vornimmt. Wurde eine binäre Signatur[261] verwendet, ist bei Ausdrucken ausschließlich die Variante der Verifikation möglich, da beispielsweise eine Rückführung von Grafiken in deren elektronisches (binäres) Original technisch nicht möglich ist. Die Behörde ist jedoch nur verpflichtet, eines der beiden Verfahren nach freiem Ermessen bereitzustellen.

Gem § 20 Satz 3 E-GovG muss das amtssignierte Dokument selbst einen Hinweis darauf beinhalten, wo im Internet (zB auf der Homepage der Behörde) sich Informationen zu den Prüfverfahren befinden. Diese Verpflichtung bezieht sich auf die Prüfung des elektronischen Dokuments, die Rückführung eines Ausdrucks einschließlich Prüfung sowie dem Verfahren zur Verifikation.[262]

12.4 Die Rechtswirkung von Ausdrucken

Seit der E-GovG-Novelle 2007[263] wird der Terminus „Auftraggeber des öffentlichen Bereichs“ statt dem der „Behörde“ verwendet, was dazu führt, dass die Amtssignatur auch in der Privatwirtschaftsverwaltung Verwendung finden kann.[264] Dadurch können auch mit Amtssignaturen versehene elektronische Rechnungen ausgestellt werden, die als solche zum Vorsteuerabzug berechtigen, sofern das der Amtssignatur zu Grunde liegende Zertifikat von einem ZDA ausgestellt wurde.[265] Der nun im E-GovG verwendete Terminus entspricht jenem des Auftraggebers des öffentlichen Bereichs gem § 5 Abs 2 DSG.[266]

[260] Erl zur RV 290 BlgNR 23. GP, 6.
[261] Bei dieser Variante wird die digitale Signatur über das gesamte Dokument (einschließlich Grafiken und sonstige Elemente) gelegt.
[262] *Rössler*, Layout Amtssignatur Spezifikation, 3.
[263] BGBl I Nr 7/2008.
[264] Erl zur RV 290 BlgNR 23. GP, 6.
[265] Vgl § 11 Abs 2 UstG iVm § 1 der Verordnung des Bundesministers für Finanzen, mit der die Anforderungen an eine auf elektronischem Weg übermittelte Rechnung bestimmt werden (BGBl II Nr 583/2003 idF Nr 175/2010).
[266] *Thienel/Schulev-Steindl*, Verwaltungsverfahrensrecht, FN 306.

Wurde ein dem Bereich der Hoheitsverwaltung entspringendes elektronisches Dokument mit einer Amtssignatur versehen, so haben Ausdrucke sowie Kopien[267] gem § 20 E-GovG die Beweiskraft einer öffentlichen Urkunde gem § 292 ZPO und *„begründen vollen Beweis dessen, was darin von der Behörde amtlich verfügt oder erklärt, oder von der Behörde oder der Urkundsperson bezeugt wird“*.[268] Inkonsistent erscheint in diesem Zusammenhang, dass § 20 E-GovG nur dem Ausdruck eines amtssignierten elektronischen Dokuments die Rechtswirkungen des § 292 ZPO zukommen lässt, nicht jedoch der elektronischen Urfassung selbst, obwohl deren Authentizität durch Prüfung der elektronischen Signatur praktisch eine viel verlässlichere Prüfung zulassen würde. Dies erscheint im Hinblick auf das Berufsrechts-Änderungsgesetz für Notare, Rechtsanwälte und Ziviltechniker 2006 – BRÄG 2006[269] umso erstaunlicher, da mit diesem Gesetz ausdrücklich auch elektronisch gefertigte Dokumente in § 292 ZPO aufgenommen wurden. Dieser Umstand wurde jedoch auch in der nach diesem Gesetz in Kraft getretenen E-GovG-Novelle 2007 nicht berücksichtigt. Obwohl es nicht unwahrscheinlich erscheint, dass dieser Umstand eventuell bei der E-GovG-Novelle 2007 übersehen wurde, geht die Regel des § 20 E-GovG als *lex specialis*[270] und auf Grund der E-GovG-Novelle 2007 auch als *lex posterior* jener des § 292 ZPO vor, wodurch tatsächlich nur Ausdrucken die Privilegierung zukommen wird. Aus den genannten Gründen erscheint eine Ausdehnung des § 20 E-GovG auch auf elektronische (amtssignierte) Dokumente sinnvoll.

12.5 Darstellung der Amtssignatur

Wie nun das Layout amtssignierter Dokumente genau gestaltet sein muss, darüber trifft das E-GovG keine konkreten Regelungen. Es sind auf Grund der gesetzlichen Bestimmungen aber jedenfalls folgende Bestandteile verpflichtend im Dokument aufzubringen:

- Bildmarke (§ 19 Abs 3 E-GovG)
- Hinweis auf die Aufbringung der Amtssignatur (§ 19 Abs 3 E-GovG)
- Verweis auf Informationen zu den Prüfverfahren (§ 20 Satz 3 E-GovG)

[267] Vgl Erl zur RV 290 BlgNR 23. GP, 6.

[268] Diese Regelung gilt nur für Ausfertigungen, die im Zuge der Hoheitsverwaltung ergehen, da an dieser Stelle ausdrücklich der Terminus „Behörde“ verwendet wird.

[269] BGBl I Nr 164/2005.

[270] Da das E-GovG nur amtssignierte öffentliche Urkunden betrifft, § 292 ZPO jedoch alle Urkunden, dürfte es sich bei der Regelung des E-GovG um lex specialis handeln.

Wo und wie diese Elemente in das Dokument eingebettet werden, steht im Ermessen der Behörde. So ist zB auch die Darstellung der Bildmarke im Briefkopf zulässig. Die aktuell am weitesten verbreitete Darstellungsvariante ist die Aufbringung eines „Signaturblocks“ am Ende des Dokuments, der alle gesetzlich geforderten Elemente beinhaltet.[271] Das empfohlene Standarddesign[272] des Signaturblocks enthält aktuell jedoch mehr Informationen als gesetzlich gefordert und teilweise auch überflüssige Elemente (zB Parameter)[273], was beim Empfänger für Unklarheiten sorgen könnte. Es ist daher empfehlenswert, lediglich die gesetzlich notwendigen und sinnvollen Elemente anzuführen.[274] Zu beachten ist in diesem Zusammenhang auch, dass es bei manchen Feldern von den konkreten Umständen abhängt, ob diese verpflichtend anzuführen sind oder nicht.[275]

Abbildung 13: Beispiel für eine minimierte Darstellung[276]
(Quelle: *Rössler*, Layout Amtssignatur Spezifikation, 8).

Aus Kostengründen und auch auf Grund der wesentlich einfacheren Administrierbarkeit ist die Verwendung des serverseitigen Signaturverfahrens zu bevorzugen. Weiters empfiehlt sich die Verwendung des Signaturblocks als Darstellungsform der Amtssignatur, jedoch auf die notwendigen Elemente reduziert. Das Layout des Signaturblocks muss diesbezüglich nur einmal im Signaturservice konfiguriert werden. Auf diese Weise kann in Folge sichergestellt werden, dass im Zuge der Aufbringung der Amtssignatur alle gesetzlich geforderten Elemente im Dokument vorhanden sind. Die entsprechende Software MOA-AS (*Module für Online-Applikationen – Amtssignatur*) steht unter der *Apache License Version 2.0*[277] kostenlos zur Verfügung und er-

[271] Vgl Beispiel auf http://www.bka.gv.at/site/cob__20071/5567/Default.aspx, abgerufen am 17. 1. 2012.
[272] *Rössler*, Layout Amtssignatur Spezifikation, 3.
[273] Dies dürfte ua auch darauf zurückzuführen sein, dass die Anzahl der vom Gesetz verpflichtend geforderten Elemente mit der E-GovG-Novelle 2007 reduziert wurde.
[274] Eine detaillierte Auflistung sämtlicher Pflicht- und Kannfelder findet sich in *Rössler*, Layout Amtssignatur Spezifikation.
[275] ZB darf der Hinweis, dass das Dokument die Beweiskraft einer öffentlichen Urkunde hat, nur auf hoheitliche Ausfertigungen aufgebracht werden oder es muss der Signaturwert dargestellt werden, wenn von der Behörde das Prüfverfahren der Rückführung in das elektronische Original gewählt wurde.
[276] Diese Darstellung ist nur dann zulässig, wenn die Verifikation als Prüfverfahren angeboten wird.

laubt auch die individuelle Konfiguration des Signaturblocks. Sie bietet im aktuellen Entwicklungsstand die Funktionalität der Aufbringung der Amtssignatur auf PDF-Dokumente sowohl in Form der textuellen als auch binären Signatur. Verwendet man darüber hinaus einen (kostenlosen) PDF-Konverter, so können amtssignierte Ausfertigungen aus nahezu jeder beliebigen Applikation erstellt werden.

13. Zusammenfassung und Ergebnisse

Die elektronische Zustellung ist eine sehr technische Rechtsmaterie und deren Regelungen finden sich an unterschiedlichsten Stellen. Basis bildet das Zustellgesetz und darauf aufbauend die Zustelldiensteverordnung, welche die Anforderungen für eine Zulassung als Zustelldienst festlegt. Diese Verordnung verweist weiter auf die technischen Spezifikationen, welche detaillierte technische Festlegungen bezüglich der Implementierung solcher Zustelldienste treffen, und erklärt diese somit als verbindlichen Bestandteil. Das Zustellgesetz selbst schreibt zwingend die Verwendung der Bürgerkarte und den Einsatz von bereichspezifischen Personenkennzeichen (bPKs) vor, wodurch auch die Regelungen des E-GovG zur Anwendung kommen. Letztendlich ermöglicht die elektronische Zustellung zusammen mit einem ELAK-System und der Amtssignatur die Abwicklung durchgehend elektronisch geführter medienbruchfreier Verwaltungsverfahren und bildet somit einen Kernteil des E-Government in Österreich.

Obwohl es sich bei den Regelungen zur elektronischen Zustellung um eine relativ neue Gesetzesmaterie handelt, konnten im Zuge der Verfassung dieser Arbeit einige Änderungs- und Verbesserungsvorschläge erarbeitet werden, welche in der nachfolgenden Tabelle übersichtlich aufgelistet werden. Insbesondere wurden Argumente identifiziert, dass die herrschende Ansicht, wonach die Durchführung des Zustellvorgangs auf Basis eines Vertrags zwischen Empfänger und Zustelldienst und nicht zwischen Behörde und Zustelldienst erfolgen sollte, weder praktisch durchführbar noch mit der Rechtslage im Einklang stehen kann.

[277] http://www.apache.org/licenses/LICENSE-2.0, abgerufen am 17. 1. 2012.

Paragraph	Alte Formulierung	Neue Formulierung	Begründung
§ 2 Z 7	Postgesetz 1997	Postmarktgesetz	Der Verweis sollte dringend aktualisiert werden (3.2.1 b).
§ 2 Z 9	Legaldefinition „Kunde“ sollte entfallen, impliziert zivilrechtliches Regelungsregime	Sollte gänzlich entfallen oder auf „Angemeldeter“ vereinheitlicht werden (2.3.5): „Person, die durch Anmeldung bei einem elektronischen Zustelldienst gem § 33 ZustG öffentlich die Willenserklärung bekannt gegeben hat, sich mit der Zustellung von elektronischen Dokumenten durch diesen Zustelldienst einverstanden zu erklären.“	
§ 8	1. Abschnitt	2. Abschnitt	Nur relevant für die physische Zustellung, nicht aber für die elektronische (4.2).
§ 29 Abs 1	„Dokumente an seine Kunden vorzunehmen“	„Dokumente entsprechend der vertraglichen Vereinbarung mit dieser an die bei ihm angemeldeten Empfänger vorzunehmen“	Dies würde zum Ausdruck bringen, dass die vertragliche Vereinbarung zwischen ZD und Behörde besteht.
§ 29 Abs 1 Z 1 lit d	-	„d) der Information, dass sich ein Kunde gem § 33 Abs. 3 abgemeldet hat“	Auch Abmeldungen müssen dem Zustellkopf gemeldet werden (4.6).
§ 29 Abs 1 lS	-	„und Z 11“	Für das Entgelt gem Z 11 sieht das Gesetz aktuell keine Regelung vor.
§ 29 Abs 1a	-	„Die der Erbringung der Zustellleistung zu Grunde liegenden Verträge werden durch erfolgreiche Übermittlung der Dokumente an die Internetadresse des Zustelldienstes oder einem anderen vom Zustelldienst festzulegenden Zugangspunkt abgeschlossen.“	Diese Regelung stellt klar, dass die Verträge über die Erbringung von Zustellungen zwischen Behörde und ZD abgeschlossen werden. Dies würde zu einer Korrektur der herrschenden (mMn nicht zutreffenden) Meinung führen, dass die Verträge zwischen Zustelldienst und Empfänger abzuschließen sind. Weiters wird auch die Form des Vertragsabschlusses definiert.
§ 32 Abs 3 (neu)	„Wurde ein Vergabeverfahren gemäß Absatz 1 erfolgreich durchgeführt oder nimmt der Übergangszustelldienst gem Absatz 2 seine Tätigkeit erneut auf, nachdem die Leistungen gemäß § 29 Abs 2 bereits von einem Ermittlungs- und Zustelldienst erbracht wurden, tritt der neu bestimmte Zustelldienst in alle bestehenden Vertragsverhältnisse ein, welche vom bisherigen Ermittlungs- und Zustelldienst im Zusammenhang mit der Erbringung der Leistungen gemäß § 29 Abs 2 abgeschlossen wurden. Jede der betroffenen Vertragsparteien kann einem solchen Vertragseintritt binnen 14 Tagen ab Übertragung der Leistungsverpflichtung widersprechen. Der neu bestimmte Zustelldienst haftet nicht für Verbindlichkeiten aus der Tätigkeit des vorhergehenden Ermittlungs- und Zustelldienstes.“		Dies würde dem Umstand begegnen, dass bei der Übertragung der Ermittlungs- und Verrechnungsleistung an eine andere juristische Person alle diesbezüglichen Verträge neu geschlossen werden müssten (9.7).
§§ 33, 35, 36	„Abgabestelle“	„Ort für Verständigungen“	Begegnet Problemen, wenn eine benannte „Abgabestelle“ keine solche iSd des § 2 Z 4 (Legaldefinition) ist (4.1.4)

Paragraph	Alte Formulierung	Neue Formulierung	Begründung
§ 33 Abs 2	-	„über ein bereitzustellendes elektronisches Verfahren“	Die Zustelldienste müssten ansonsten Datenänderungen akzeptieren, die physisch per Post übermittelt wurden (4.5).
§ 34 Abs 2 2. Satz		„, im zweiten Fall anstatt des bPK gem § 6 E-GovG jenes gem § 14 E-GovG.“	Das bPK gem § 6 E-GovG kann im Fall einer Privatzusendung nicht als Suchkriterium herangezogen werden.
§ 1 Abs 1 E-GovG	„[…] Kommunikationsarten für Anbringen an diese Stellen“	„Kommunikationsarten mit diesen Stellen“	Die Wahlfreiheit besteht auch für Zustellungen und nicht nur für Anbringen (3.2.4).
§ 20 E-GovG	Einschränkung der Beweiskraft lediglich auf Ausdrucke amtssignierter Dokumente.		Sollte im Hinblick auf § 292 ZPO neu auch auf elektronische amtssignierte Dokumente ausgedehnt werden (12.4).

Literatur und Referenzen

Aichholzer, Georg / Schmutzer, Rupert: E-Government in Österreich in *Schweighofer et al. (Hrsg):* E-Commerce und E-Governmnet. Verlag Österreich Wien 2000. ISBN 3-7046-1592-7.

Apathy, Peter / Riedler, Andreas: Bürgerliches Recht III[4]. Springer Verlag Wien, 2010. ISBN 978-3-211-99426-9.

Barta, Heinz: onlineLehrbuch Zivilrecht, http://www.uibk.ac.at/zivilrecht/buch, zuletzt abgerufen am 17. 1. 2012.

Bauer, Lukas / Reimer, Sebastian: Handbuch Datenschutzrecht. Facultas.wuv Wien, 2009. ISBN 978-3-7089-0509-9.

Bengel, Günther: Grundkurs Verteilte Systeme[3].Vieweg Verlag Wiesbaden, 2004. ISBN 3-528-25738-5.

Bitzer, Farnk / Brisch, Klaus M.: Digitale Signatur. Springer Verlag Berlin Heidelberg, 1999. ISBN 3-540-65563-8.

BKA, Grundlagen zum österreichischen E-Government Gütesiegel, http://www.bka.gv.at/DocView.axd?CobId=28023, abgerufen am 17. 1. 2012.

Brenn, Christoph: Signaturgesetz. Manz Verlag Wien, 1999. ISBN 3-214-04132-0.

Bydlinski, Peter: Bürgerliches Recht I[5]. Springer Verlag Wien, 2010. ISBN 978-3-211-99436-8.

Connert, Wilfried: Das „E-Government-Gesetz“ – ein Überblick. Gemeindezeitung 3/2004.

Connert, Wilfried: Rechtsgrundlagen für das elektronische Verfahren und den ELAK in *Schweighofer et al. (Hrsg):* Zwischen Rechtstheorie und e-Government. Verlag Österreich Wien 2003. ISBN 3-7046-4091-3.

Coulouris, George / Dollimore, Jean / Kindberg, Tim: Verteilte Systeme. Konzepte und Design. Pearson Education Deutschland GmbH München, 2002. ISBN 3-8273-7022-1.

Dohr, Walter / Pollirer, Hans-Jürgen / Weiss, Ernst: E-Government-Gesetz. Manz Verlag Wien, 2004. ISBN 3-214-08672-3.

Dohr, Walter / Pollierer Hans-Jürgen: Datenschutzkonforme Organisation, ecolex 2006, 706.

Doralt, Werner (Hrsg): Kodex Verwaltungsverfahrensgesetze[36]. LexisNexis Verlag Wien, 2008. ISBN 978-3-7007-3749-0.

Drobesch, Heinz / Grosinger, Walter: Das neue österreichische Datenschutzgesetz. Juridica Verlag Wien, 2000. ISBN 3-85131-128-0.

Dullinger, Silvia: Bürgerliches Recht II[4]. Springer Verlag Wien, 2010. ISBN 978-3-211-99450-4.

Duschanek, Alfred / Rosenmayr-Klemenz, Claudia: Datenschutzgesetz 2000. Wirtschaftskammer Österreich Wien, 2000. ISBN 3-902110-00-7.

Feil, Erich: Zustellwesen[5]. Linde Verlag Wien, 2006. ISBN 3-7073-0876-6.

Grabler, Hermann: Kommentar zur GewO. 3. Auflage. Springer Verlag Wien 2011. ISBN 978-3-211-88730-1.

Graf, Wolfgang: Datenschutzrecht im Überblick. Facultas Verlag Wien 2004. ISBN 3-85114-835-5.

Hengstschläger, Johannes: Verwaltungsverfahrensrecht[4]. Facultas.WUV Wien, 2009. ISBN 978-3-7089-0283-8.

Hollosi, Arno / Hörbe, Rainer: Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen. Version 1.1.1. http://portal.bmi.gv.at/ref/portref/files/anleitungen/Stammzahl-bPK-Algorithmen.doc, zuletzt abgerufen am 17. 1. 2012.

Holzinger, Gerhart: Die Organisation der Verwaltung in *Holzinger/Oberndorfer/Raschauer:* Österreichische Verwaltungslehre[2]. Verlag Österreich Wien 2006. ISBN 3-7046-4786-1.

Horn, Bernhard / Trabitsch, Roman / Fischer, Gerald / Grechenig Thomas: Die Amtssignatur in Gemeinden – Ein erster Erfahrungsbericht, *Schweighofer, Erich / Kummer, Franz (Hrsg)*: Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts (2011), ISBN 978-3-85403-278-6.

Horn, Bernhard / Trabitsch, Roman / Fischer, Gerald / Grechenig Thomas: Die elektronische Zustellung aus Sicht der Versendung, *Schweighofer, Erich (Hrsg)*: Sicherheit und proaktiver Staat im ökonomischen Kontext, Österreichische Computer Gesellschaft, (2010), ISBN 978-3-85403-226-3.

Jahnel, Dietmar: Datensicherheitsmaßnahmen nach dem DSG. http://www.internet4jurists.at/literatur/datensicherheit.pdf, zuletzt abgerufen am 17. 1. 2012.

Jahnel, Dietmar (Hrsg): Datenschutzrecht und E-Government. NWV Neuer Wissenschaftlicher Verlag Wien Graz, 2008. ISBN 978-3-7083-0529-5.

Karlinger, Gregor: Allgemeine Richtlinien für Amtssignaturzertifikate in der Verwaltung, http://reference.e-government.gv.at/Amtssignaturzertifikate.1095.0.html, zuletzt abgerufen am 17. 1. 2012.

Karning, Bernhard: Rechtliche Aspekte des E-Government in Österreich. WiKu-Verlag Berlin, 2004. ISBN 3-86553-123-7.

Karning, Bernhard / Kustor, Peter: E-Government. In *Bauer/Reimer*, Handbuch Datenschutzrecht, Facultas.wuv Wien, 2009. ISBN 978-3-7089-0509-9.

Koziol, Helmut / Welser, Rudolf / Kletecka, Andreas: Bürgerliches Recht I[13]. Manz Verlag Wien, 2006. ISBN 3-214-14708-0.

Kunstein, Florian: Die elektronische Signatur als Baustein der elektronischen Vewaltung. Tenea Verlag Bistrol Berlin, 2005. ISBN 3-86504-123-X.

Laga, Gerhard / Sehrschön, Ulrike / Ciresa, Meinhard: E-Commerce Gesetz. Lexis-Nexis ARD Orac Wien , 2007. ISBN 978-3-7007-3713-1.

Laga, Gernhard / Reissner, Christoph: Sicherer elektronischer Geschäftsverkehr. Obersteirische Druckerei Leoben, 2000.

Larcher, Albin: Zustellrecht. Manz Verlag Wien, 2010. ISBN 978-3-214-00680-8.

Makolm, Josef: E-Government-Gesetz und Interoperabilität in *Schweighofer et al. (Hrsg):* Effizienz von e-Lösungen in Staat und Gesellschaft. Verlag Österreich Wien 2005. ISBN 3-415-03615-4.

Mayer-Schönberger, Viktor / Brandl, Ernst O.: Datenschutzgesetz 2000. Linde Verlag Wien, 1999. ISBN 3-85122-983-5.

Mayer-Schönberger, Viktor / Brandl, Ernst O.: Datenschutzgesetz[2]. Linde Verlag Wien, 2006. ISBN 3-7073-0869-3.

Mayer-Schönberger, Viktor: Signaturgesetz. Orac Verlag Wien, 1999. ISBN 3-7007-1754-7.

Österreichische Computer Gesellschaft: Behörden im Netz. Ueberreuter Print & Digimedia GmbH Wien, 2006. ISBN 3-85403-205-6.

Österreichische Computer Gesellschaft: Semantisches Web und Soziale Netzwerke im Recht, Tagungsband des 12. Internationalen Rechtsinformatik Symposions IRIS 2009, OCG-Verlag Wien, 2010. ISBN 978-3-85403-259-5.

Öhlinger, Theo: Verfassungsrecht[7]. Facultas Verlag Wien 2007. ISBN 987-3-7089-0152-7.

Parycek, Peter: E-Government: Terminologie und Konzeption eines rechtlichen Modells in *Schweighofer (Hrsg) et al:* e-Staat und e-Wirtschaft aus rechtlicher Sicht. Verlag Österreich Wien 2006. ISBN 978-3-415-03767-0.

Pollirer, Hans-Jürgen / Weiss, Ernst / Knyrim, Rainer: DSG. Manz Verlag Wien, 2010. ISBN 978-3-214-13401-3.

Posch, Reinhard / Payer Udo: Automatische Authentifizierung mittels Bürgerkarte in S*chweighofer et al. (Hrsg):* IT in Recht und Staat. Verlag Österreich Wien 2002. ISBN 3-7046-3827-7.

Projektgruppe "Amtssignatur": Amtssignatur 2008 Leitfaden und best practise. http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=35263, zuletzt abgerufen am 17. 1. 2012.

Raschauer, Bernhard: Allgemeines Verwaltungsrecht[2]. Springer Verlag Wien New York, 2003. ISBN 3-211-40540-2.

Raschauer, Nicolas / Sander, Peter / Wessely Wolfgang (Hrsg.): Österreichisches Zustellrecht. Springer Verlag Wien New York, 2007. ISBN 978-3-211-69917-1.

Reichstädter, Peter / Tauber, Arne / Hollosi, Arno: Modell und Prozesse der elektronischen Zustellung (ZUSEMOD 1.3.1).

http://reference.e-government.gv.at/Zustellung.351.0.html, zuletzt abgerufen am 17. 1. 2012.

Reichstädter, Peter / Rössler, Thomas / Tauber, Arne: Modell und Prozesse der Zustellungs-Verrechnung (ZUSERECH 1.3.2).
http://reference.e-government.gv.at/Zustellung.351.0.html, zuletzt abgerufen am 17. 1. 2012.

Riedl, Reinhard: Digitale Identität und Datenschutzanforderungen an IT-Lösungen im E-Government in *Schweighofer et al. (Hrsg):* Zwischen Rechtstheorie und e-Government. Verlag Österreich Wien 2003. ISBN 3-7046-4091-3.

Rössler, Thomas / Tauber, Arne / Reichstädter, Peter: Elektronische Zustellung – Message Spezifikation (ZUSEMSG, 1.3.0).
http://reference.e-government.gv.at/Zustellung.351.0.html, zuletzt abgerufen am 17. 1. 2012.

Rössler, Thomas / Karning, Bernhard: Spezifikation Layout Amtssignatur.
http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=35264, zuletzt abgerufen am 17. 1. 2012.

Seböck, Walter: E-Government – Elektronische Verwaltung. Dissertation an der Universität Wien 2005.

Schweighofer, Erich / Geist, Anton / Staufer, Ines (Hrsg.): Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik. Tagungsband des 13. Internationalen Rechtsinformatik-Symposions IRIS 2010. books@ocg.at Wien, 2010.

Schreiber, Lutz: Elektronisches Verwalten. Nomos Verlag Baden-Baden, 2003.

Steiner, Wolfgang: Die elektronische Verfahrensführung nach dem AVG – Rechtslage und erste Erfahrungen in *Schweighofer et al. (Hrsg):* Zwischen Rechtstheorie und e-Government. Verlag Österreich Wien 2003. ISBN 3-7046-4091-3.

Tauber, Arne / Rössler, Thomas / Reichstädter, Peter: Elektronische Zustellung – Technische Spezifikation (ZUSESPEC 1.3.1).
http://reference.e-government.gv.at/Zustellung.351.0.html, zuletzt abgerufen am 17. 1. 2012.

Tauber, Arne / Rössler, Thomas: Elektronische Zustellung – Zustellkopf (ZUSEKOPF 1.3.2). http://reference.e-government.gv.at/Zustellung.351.0.html, zuletzt abgerufen am 17. 1. 2012.

Tauber, Arne / Reichstädter, Peter: Elektronische Zustellung – LDAP Schemabeschreibung (ZUSELDAP 1.3.2).
http://reference.e-government.gv.at/Zustellung.351.0.html, zuletzt abgerufen am 17. 1. 2012.

Tauber, Arne / Rössler, Thomas / Reichstädter, Peter: Elektronische Zustellung – Nachweisliche Zusendung im Auftrag von Privaten (ZUSEPRIV, 1.3.1).
http://reference.e-government.gv.at/Zustellung.351.0.html, zuletzt abgerufen am 17. 1. 2012.

Tauber, Arne: Elektronische Zustellung – Push Protokoll (ZUSEPUSH, 1.3.2).
http://reference.e-government.gv.at/Zustellung.351.0.html, zuletzt abgerufen am 17. 1. 2012.

Thienel, Rudolf: Verwaltungsverfahrensrecht[5]. Verlag Österreich Wien 2009. ISBN 978-3-7046-5409-0.

Thienel, Rudolf: Aktuelle Entwicklungen des E-Government in Österreich. http://www.rechtsprobleme.at/doks/thiele-egovernment.pdf, zuletzt abgerufen am 17. 1. 2012.

Trauner, Gudrun: E-Government in *Holzinger/Oberndorfer/Raschauer:* Österreichische Verwaltungslehre[2]. Verlag Österreich Wien 2006. ISBN 3-7046-4786-1.

Walter, Robert (Hrsg): Die österreichischen Verwaltungsverfahrensgesetze[17]. Manz Verlag Wien, 2008 . ISBN 978-3-214-03255-5.

Welser, Rudolf: Bürgerliches Recht II[13]. Manz Verlag Wien, 2007. ISBN 978-3-214-14709-9.

Wimmer, Maria A.: E-Government im Trend der Verwaltungsinformatik in *Schweighofer et al. (Hrsg):* Auf dem Weg zur ePerson. Verlag Österreich Wien 2001. ISBN 3-7046-1719-9.

Zankl, Wolfgang: Bürgerliches Recht. Facultas.wuv Wien, 2010. ISBN 978-3-7089-0570-9.

Zankl, Wolfgang: E-Commerce-Gesetz: Kommentar und Handbuch. Verlag Österreich Wien, 2002. ISBN 3-7046-3685-1.

Zankl, Wolfgang: Qualifikation und Dauer von Mobilfunkverträgen, ecolex 2005, 29.

Zankl, Wolfgang: Rechtsqualität und Zugang von Erklärungen im Internet, ecolex 2001, 344.

Zörner, Stefan: LDAP für Java-Entwickler[3]. entwickler.press Siegen, 2008. ISBN 978-3-939084-07-5.

Abkürzungsverzeichnis

aA	anderer Ansicht/Auffassung
Abs	Absatz
aF	alte Fassung
Art	Artikel
AVG	Allgemeines Verwaltungsverfahrensgesetz 1991
BArchG	Bundesarchivgesetz
BGBl	Bundesgesetzblatt
BKA	Bundeskanzleramt
BMF	Bundesminister(ium) für Finanzen
BMI	Bundesminister(ium) für Inneres
bPK	bereichsspezifisches Personenkennzeichen
bzw	beziehungsweise
ca	circa
dh	das heißt
DSK	Datenschutzkommission
EB	Erläuternde Beilagen
E-GovG	E-Government-Gesetz
E-Gov-BerAbgrV	E-Government-Bereichsabgrenzungsverordnung
ELAK	Elektronischer Akt[278]
etc	et cetera
f	der/die folgende
ff	fortfolgende
FN	Fußnote
gem	gemäß
hL	herrschender Lehre
idF	in der Fassung
idR	in der Regel
idZ	in diesem Zusammenhang
IKT	Informations- und Kommunikationstechnologie
insb	insbesondere

[278] Nicht zu verwechseln mit dem Projekt „ELAK im Bund“.

iSd	im Sinne des
iSv	im Sinne von
iVm	in Verbindung mit
lit	litera
lS	letzter Satz
mE	meines Erachtens
mMn	meiner Meinung nach
mwN	mit weiteren Nachweisen
nF	neue Fassung
PMG	Postmarktgesetz
RL	Richtlinie
RN/RZ	Randnummer/Randziffer
RV	Regierungsvorlage
SigG	Signaturgesetz
SigV	Signaturverordnung
StZRegV	Stammzahlenregisterverordnung
ua	unter anderem
uU	unter Umständen
va	vor allem
vgl	vergleiche
VO	Verordnung
VwGH	Verwaltungsgerichtshof
Z	Ziffer
zB	zum Beispiel
ZDA	Zertifizierungsdiensteanbieter
ZFormV	Zustellformularverordnung
ZMR	Zentrales Melderegister
ZustG	Zustellgesetz

Anhang I: Abstract

Diese Arbeit beschäftigt sich mit der Thematik der rechtsverbindlichen Elektronischen Zustellung behördlicher Dokumente, wofür unterschiedliche Verfahren zur Anwendung kommen können. Der Großteil der einschlägigen rechtlichen Regelungen findet sich im Zustellgesetz (ZustG), insbesondere im 3. Abschnitt, aber auch Regelungen des E-GovG, SigG, DSG 2000 und des ECG können in diesem Zusammenhang einschlägig sein. Es werden einerseits die rechtlichen Rahmenbedingungen erläutert und gewisse sich daraus ergebende Fragestellungen diskutiert, andererseits werden die sich daraus ergebenden technischen Implikationen erörtert. Für eine elektronische Zustellung von behördlichen Dokumenten durch einen elektronischen Zustelldienst ist dessen vorherige Zulassung durch das BKA erforderlich, wobei im Zuge des Zulassungsverfahrens geprüft wird, ob die entsprechenden Anforderungen der Zustelldiensteverordnung (ZustDV) erfüllt und die verwiesenen technischen Spezifikationen implementiert wurden, welche von der IT-Kooperation Bund-Länder-Gemeinden (http://reference.e-government.gv.at/Zustellung.351.0.html) verbindlich festgelegt wurden. Diese Spezifikationen werden gem § 3 Abs 1 Z 7 iVm Anlage 1 ZustDV zu einem normativern Bestandteil der Verordnung erklärt. Ziel dieser Arbeit ist es, einem Juristen die gesetzlichen Regelungen der Elektronischen Zustellung behördlicher Dokumente näher zu bringen und die damit verbundenen technischen Hintergründe und Konzepte zu erläutern. Es soll ein Verständnis dafür geschaffen werden, wie die einzelnen Normen in der Praxis technisch umgesetzt und erfüllt werden können.

Im Zuge der Arbeit werden die einzelnen Arten der Elektronischen Zustellung im Verwaltungsverfahren (ZustG) einer detaillierten Beleuchtung unterzogen, insbesondere die Zustellung unter Einsatz eines zugelassenen Zustelldienstes sowie die Zustellung an eine elektronische Zustelladresse. Dies umfasst auch die rechtlichen Regelungen bezüglich der Anmeldung bei einem Zustelldienst als Empfänger und der Erbringung der Zustell-, Ermittlungs- und Verrechnungsleistung durch einen zugelassenen Zustelldienst. Im Zuge dessen werden die aktuell zum Einsatz kommenden Technologien und konkreten technologischen Umsetzungen erklärt und so der Konnex zwischen Recht und Technik hergestellt.

Auch die rechtlichen und technischen Aspekte der Anbindung von Behörden (oder Privaten) an das gesamte Zustellsystem werden dargelegt und ausführlich erklärt. Besonderes Augenmerk soll hier auf die Rechtsverhältnisse zwischen den Akteuren, insbesondere jene zwischen Behörde und einen durch sie in Anspruch genommenen Zustelldienst sowie zwischen Zustelldienst und potentiellem Empfänger, gelegt werden. Hier wird auch der Beweis erbracht, dass die Anmeldung bei einem elektronischen Zustelldienst durch einen potentiellen Empfänger lediglich eine Einwilligung gem § 1 Abs 1 E-GovG in eine elektronische Kommunikation darstellt, welche als öffentlich-rechtliche Erklärung zu qualifizieren ist, nicht aber ein zivilrechtlichen Vertrag begründet.

Weiters beschäftigt sich diese Arbeit mit den rechtlichen Anforderungen an elektronische behördliche Dokumente, welche erfüllt sein müssen, damit solchen Dokumenten Rechtsverbindlichkeit zukommt. Dies umfasst Aspekte der elektronischen Signatur als Pendant zur herkömmlichen Unterschrift und die Sicherstellung der Authentizität behördlicher Dokumente durch Aufbringung einer Amtssignatur. Dazwischen werden an passender Stelle immer wieder datenschutzrechtliche Aspekte und Fragestellungen erörtert.

Weiters kann der Bürger auch in den Empfang elektronischer Dokumente von Privaten einwilligen. Dies erfolgt technisch idR durch Aktivierung einer Checkbox. Genau diese Aktivierung stellt aber den Abschluss eines zivilrechtlichen Vertrags in der Form eines Hostingvertrags gem § 16 ECG für elektronische Nachrichten sowie Dokumente dar. Hieraus ergeben sich eine Reihe rechtlicher Fragestellungen, die in der Arbeit erörtert und diskutiert werden. Diesbezüglich wird auch eine klare Abgrenzung der rechtlichen Regelungen zur hoheitlichen Zustellung und der privatrechtlichen Zusendung von Dokumenten gezogen.

Die abschließende Zusammenfassung bietet einen Überblick über alle relevanten Punkte und gezogene Erkenntnisse.

Anhang II: Curriculum Vitae

MMag. Dipl.-Ing. Bernhard Horn

BESCHÄFTIGUNG	Projektassistent
März 2009 – ongoing	**Research Industrial Systems Engineering (RISE) GmbH**
Beruf oder Funktion	Projektarbeit, Legal & Compliance
Wichtigste Tätigkeiten	Datenschutz, IT/IP-Recht, E-Government-Recht, Medizinprodukterecht
März 2009 – ongoing	**Technische Universität Wien**
Beruf oder Funktion	Wissenschaftlicher Mitarbeiter
Wichtigste Tätigkeiten	Mitwirkung an der Lehrveranstaltung „Management von Software Projekten“ Forschungstätigkeit im Bereich E-Government: E-Government-Recht, E-Government-Technologien
BERUFSERFAHRUNG	
Oktober 2007 – Juni 2011	**Juranovit Forschungs GmbH** **europäisches zentrum für e-commerce und internetrecht (www.e-center.eu)**
Beruf oder Funktion	Key Account Assistent, wissenschaftlicher Mitarbeiter
Wichtigste Tätigkeiten	Verfassung diverser wissenschaftlicher Stellungnahmen zu Themen des IT-Rechts Laufendes Reporting über aktuelle Rechtsentwicklungen Mitarbeit an der Publikation: *Zankl (Hrsg)*, Auf dem Weg zum Überwachungs-staat?, facultas wuv, 2009.
Branche	Internet- und Telekommunikationsrecht
SCHUL- UND BERUFSBILDUNG	
März 2009 – ongoing	**Doktoratsstudium Rechtswissenschaft (Dr. jur.)** Universität Wien Schwerpunkte: E-Government-Recht, Technologierecht, Wirtschaftsrecht, IT-Recht
März 2005 – März 2009	**Masterstudium Wirtschaftsinformatik (Mag. rer. soc. oec.)** Interdisziplinäres Studium an der Technischen Universität Wien und Universität Wien Schwerpunkt: Projekt- und Qualitätsmanagement Abschluss mit ausgezeichnetem Erfolg

Oktober 2005 – Jänner 2009	**Masterstudium Software Engineering & Internet Computing (Dipl.-Ing.)**
	Technische Universität Wien
	Schwerpunkt: Wirtschaft und Management
	Abschluss mit ausgezeichnetem Erfolg
Oktober 2001 – Jänner 2008	**Diplomstudium Rechtswissenschaft (Mag. jur.)**
	Universität Wien
	Schwerpunkte: Rechtsinformatik, IKT-Recht, Europarecht
Oktober 2001 – März 2005	**Bachelorstudium Wirtschaftsinformatik (Bakk. rer. soc. oec.)**
	Interdisziplinäres Studium an der Technischen Universität Wien und Universität Wien
	Schwerpunkt: Vernetzte Systeme
	Abschluss mit ausgezeichnetem Erfolg
Oktober 2000 – Mai 2001	**Präsenzdienst Pionierbataillon II Salzburg**
September 1995 – Juni 2000	**HTL-Leonding** (Ausbildungszweig EDV & Organisation)

PUBLIKATIONEN

B. Horn, G. Fischer, R. Trabitsch, T. Grechenig: An Outline of the Technical Requirements on Governmental Electronic Record Systems Derived from the European Legal Environment, *M. Klun, M. Decman, T. Jukic (eds.):* Proceedings of the 11th European Conference on e-Government (2011), ISBN 978-1-908272-01-0 CD.

B. Horn, T. Grechenig: Cloud Computing in der Medizin – Patientengeheimnis versus medizinischer Fortschritt, *E. Schweighofer, F. Kummer (eds.):* Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts (2011), ISBN 978-3-85403-278-6 (nominiert beim Best-10-Paper-Award).

B. Horn, R. Trabitsch, G. Fischer, T. Grechenig: Die Amtssignatur in Gemeinden – Ein erster Erfahrungsbericht, *E. Schweighofer, F. Kummer (eds.)*: Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts (2011), ISBN 978-3-85403-278-6.

B. Horn, G. Fischer, R. Trabitsch, T. Grechenig: Die elektronische Zustellung aus Sicht der Versendung, E. *Schweighofer (ed.)*: Sicherheit und proaktiver Staat im ökonomischen Kontext, Österreichische Computer Gesellschaft, (2010), ISBN 978-3-85403-226-3.

B. Horn, G. Fischer, R. Trabitsch, T. Grechenig, J. Wachter: Technische und systemische Implikationen der österreichischen Rechtslage für ein ELAK-System in der öffentlichen Verwaltung, E. *Schweighofer (ed.)*: Semantisches Web und Soziales Web im Recht, Österreichische Computer Gesellschaft, (2009), ISBN: 978-3-85403-259-5; 153 - 158.

T. Wild, T. Hölzenbein, T. Grechenig, M. Bernhart, A. Binder, B. Horn, S. Strobl, J. Unosson, M. Prinz, A. Wujciow: "Digitale Wunddiagnostik und -dokumentation mit W.H.A.T. als Basis für eine integrative Versorgung";

Wundmanagement, 06 (2009).

B. Horn: Die Online-Durchsuchung, Output 2/2008.