AUSTRIAN STATE RECORDS MANAGEMENT LIFECYCLE

Berthold Konrath
Austrian State Archives
Nottendorfer Gasse 2
A-1030 Vienna
Austria

Robert Sharpe
Tessella
26 The Quadrant
Abingdon Science Park
Abingdon OX14 3YS
United Kingdom

ABSTRACT

The Austrian state is building an integrated "cradle to grave" electronic records management and archive process to ensure that electronic records are managed correctly throughout their lifetime.

This has already included the rollout of records management through federal agencies via the ELAK (Elektronisher Akt) system and the specification of a format for transfer between agencies called EDIAKT. The latter includes transfer to the national archives and thus, in essence, the definition of the format of a valid SIP that can be ingested into an archival system.

The Austrian Federal Chancellery is now funding the provision of such a central archival system plus a general license allowing all Austrian public bodies to benefit from the technology for archiving and preservation. After a competitive tender, Siemens IT Solutions & Systems are providing this system utilising the Safety Deposit Box (SDB) system from Tessella.

This system will ingest the SIPs (in EDIAKT format) into long-term storage and provide comprehensive access, data management, preservation and administration functions. The Österreichische Staatsarchiv (Austrian State Archives) will be the first to use this system by the end of 2010.

This is the basis on which the requirements for maintaining electronic records, which will be the sources of historical research in the future, are being created. This will preserve the historical heritage of Austria for generations to come.

1. INTRODUCTION

The impact of modern technology (computers, mobile phones, the Internet etc.) has been felt throughout our daily lives for some time now. As part of this trend there has been a huge impact on government departments and consequentially on government records. This has spawned new phrases such as "e-government" which in some ways has become a synonym for a modern state. However, this exciting trend also throws up challenges and it forces records mangers and archivists to have new processes.

For years, and increasingly so in the recent past, modern administrations have used IT-instruments in the fulfilment of their statutory tasks. As early as in 1985, the Austrian Archiv der Republik (the part of the Austrian State Archives [1] responsible for records post 1918) introduced an electronic file administration system. In 2003 the Austrian State Archives were among the first Austrian federal services to change over to the exclusive use of electronic files.

In Austria, the long-term storage of electronic data from both electronic file administration systems and other systems as well as the acceptance of "traditional hard copies" are responsibilities of the Archiv der Republik. In this context, experts from the Archiv der Republik have, from the very start, been involved in the introduction of the "paperless office" (use of federal electronic files), the management of electronic files (Document Lifecycle Management) and the creation of an electronic interface (EDIAKT II) between the different electronic filing systems of the Austrian federal administration.

More recently, a feasibility study was undertaken in 2006-7 to define requirements, possible solutions, conventions and categories for a digital long-term archive. One of the key requirements was that the system needed to be compatible with key international standards especially OAIS. This led to a clear need for cooperation between the Austrian State Archives and the Austrian Federal Chancellery in order to procure the system called Digitale Langzeitarchivierung im Bund (DigLAimBund) based on these requirements.

This led to a public tender which was won by Siemens IT Solutions & Services together with their software partner Tessella utilising the Safety Deposit Box (SDB) system which, in conjunction with appropriate hardware and other systems, constitutes an OAIS-complaint solution. This system will be used by the Österreichische Staatsarchiv (Austrian State Archives) and other agencies in order to ensure the preservation of electronic records for the next generation.

2. FEDERAL RECORDS MANAGEMENT

As experience has too often shown, paper files can be lost, misplaced, incorrectly filed, or land in a back corner of the archives. Hence, one of the most important developments of eGovernment for the Government is the electronic record system, called ELAK. It enables seamless communication between public authorities and other governmental services.

In 2001, the ELAK ("Elektronischer Akt) system for records management was launched department-wide in the Austrian Ministry for Foreign Affairs and the Federal Chancellery. Since then, ELAK has been rolled out nation-wide and is also being introduced step by step in provincial governments.

The advantages of electronic record processing are obvious. ELAK substantially reduces the amount of time required for processing applications since documents no longer need to be sent back and forth between ministries and public authorities. Instead, they can be processed conveniently online. Processes are standardized and can run parallel to one another. Enquiries can be carried out directly from the desktop and the process workflow is completely transparent. With practically just a push of a button you can find out at any time of day how far the file has been processed. Furthermore, there are never any problems due to changes in the format of the file (printed copies, scans) because ELAK is based on a standardized system with uniform user interfaces. The days of traditional paper-oriented file processing are numbered. In the meantime, paper-oriented file processing is being replaced by automated business processes.

In their function as a document and workflow management system for the electronic implementation of internal work processes, electronic file systems become a kind of data hub in which different applications and data sources can be integrated so that changes in media format can be avoided. In the electronic record system of the federal administration, the most important interfaces and systems for public administration are:

- Form server: This interface displays forms in graphical user interfaces, making it the most important interface from the citizen's point of view. Application forms that are submitted over a Web form can be processed directly in the ELAK system due to their standardized data structure and XML syntax.
- Electronic delivery: In order to transmit information, notices, and documents to the intended person, the piece of correspondence must be delivered via a delivery service using the methods described.
- Interfaces to other applications: information is often needed from citizens during procedures which they are not able to supply, either because it would require too much effort, or because it may not be possible for the citizen to do so. Instead of citizens having to chase their data around, the data should be able to be accessed by the ELAK system in an automated manner from public administration applications such as registers, SAP systems or directory services. Communication occurs over defined interfaces that support the standardized exchange of data.

The Austrian eGovernment strategy requires active participation in creating interfaces which are standardized across public authorities and drafting specifications that are effective nationwide as part of the cooperation between the Federal Government, the provinces and municipalities. The results from the work groups are based wherever possible on international norms and standards, or use them as a model. The typical eGovernment components that are needed in administrative and back-office processes join together to form a big picture. Along with individual applications, the big picture includes modules for online applications and components of the citizen card concept. The protocols used in the communication architecture function figuratively as the mortar that holds the building blocks together.

3. DEFINING SIPS USING EDIAKT

The ability of government agencies to use and manage electronic records is just a start. It is also necessary for these agencies to exchange information with each other. Although all such agencies have record management systems that work with electronic records, records of business processes, and sub- processes including documents, the objects were specific to the manufacturer of the software and not built according to a uniform standard. To this end, EDIAKT [2] was developed as a format for standardising communication between different public institutions (authorities, courts of law, businesses).

In the course of further development of the EDIAKT system and due to increased distribution of the ELAK system, the standard was updated to its current format, EDIAKT II.

In this standard, data is packaged as EDIAKT objects, which are comprised of:

- Meta-data that describes a record, business (sub-) process, or document
- Process data for process instances and activities in accordance with the XPDL standard of the Workflow Management Coalition
- Content of the record, business (sub-)process, or document
- Procedure-specific data that may be attached to an object.

To satisfy the different requirements of institutions using ELAK, EDIAKT implemented a hierarchical structure with four layers. At the bottom is the document, which contains the file in its original format. If the file is not saved in a standard format, a document with a standard format must be attached. One or more documents are encapsulated in a record of a business sub-process. It represents the smallest object in EDIAKT II. This business sub-process may further be aggregated along with other sub-process in a higher-level business process record. Authorities that do not have their own ELAK system can still read EDIAKT packages using the free EDIAKT Viewer. The current version can be used to:

- Display all meta-data including process data,

- Show embedded documents,
- Verify digital signatures.

EDIAKT II is used more than just as an interface between different electronic record systems. It can also be used for internal data exchange between special applications and archive systems. EDIAKT II, together with the EDIAKT Viewer and EDIAKT Creator, and supplemented by the standard document format PDF/A, establishes the basis for the long-term archiving of records. In the future, this format could play an increasingly central role for the submission of original records that is required for different courts of jurisdiction.

4. DigLAimBUND OVERVIEW

Once government records have reached the end of their operational life within the original creating agency (and other related or successor agencies) they need to be assessed to see if they need to be retained for a longer time period. A proportion of those retained will indeed eventually be selected for permanent retention at the Österreichische Staatsarchiv (Austrian State Archives) and will thus be transferred to them.

This requires the Austrian State Archives to have a system that is capable of ingesting, storing, managing, preserving and providing access to these records. This is the role of the Digitale Langzeitarchivierung im Bund (DigLAimBund).

DigLAimBund is based on the pre-existing SDB4 system. This system is a Java web-based server application running with a relational database (in this case Oracle) behind it. When combined with operational hardware, a physical storage system and a system for authorisation and authentication, it offers all the functions required of an OAIS system. In the following sections for the rest of the paper each of the functions of each of the functional entities in OAIS are discussed in turn illustrating how DigLAimBund complies with this.

One of its key features is its “Active Preservation” module that allows automated, verifiable digital preservation to occur controlled by a Technical Registry. The Technical Registry is another Java web-based server application with a relational database behind it. It is based on the Planets Core Registry [3] that is itself based upon the UK National Archive’s PRONOM system [4,5]. The Technical Registry contains not just factual information (e.g., a list of formats, known software, migration pathways etc.) but also policy information (e.g., which formats or combination of formats and properties are considered to make a file obsolete and thus in need of preservation action, how to measure these properties, which preservation action to perform in which circumstances etc.). This policy is machine-readable which is the key to allowing digital preservation to be automated.

Another feature is that it contains a built-in workflow system, which is based on Drools Flow (an open-source development). This allows configurable workflows to be created with comparative ease for each OAIS processes. Each workflow consists of a series of workflow steps. These steps can be automated steps or can involve user input (via a web form). Each step is self-recording so that an audit trail of actions is created.

5. DigLAimBUND INGEST

The first ingest function defined in OAIS is the ability to receive a submission. Clearly this requires a government agency to transfer a SIP in the EDIAKT II format to the archive.

5.1. Receive Submission

Once the physical transfer has taken place, it needs to pass into the boundary of the DigLAimBUND system. The first step to be performed is to transform the EDIAKT package into a format that is understood by the archiving system. This allows the SIPs to then be converted to AIPs in such as way as to utilise standard ingest, storage, access, data management and preservation workflow steps already present in SDB. This restricts the amount of development needed within the project to those aspects needed for genuinely local configuration or enhancements.

In the case of SDB, it utilises a metadata schema called XIP (that covers SIPs, AIPs and DIPs). This schema defines the structural metadata needed to link records to files in given manifestations. This is especially important for EDIAKT II since it is normal to receive both an original and a normalised form of each record (e.g., Word and PDF documents). In addition, the XIP schema defines technical metadata. In particular, it has been specifically designed to allow the automation of digital preservation (see below). However, XIP does not proscribe descriptive metadata, instead allowing descriptions to be described using any appropriate metadata schema (e.g., EAD), which can be embedded inside XIP.

5.2. Perform Quality Assurance

Next the “perform quality assurance” steps required by OAIS are performed. This includes virus checking, verifying compliance with schemas, fixity value checks and a check that every entity’s identifier is unique.

5.3. Generate AIP

The next step is to generate the AIP. As described above, XIP allows this to happen through gradual refinement but one of the key steps involved is characterisation.

In SDB characterisation is itself a multi-stage process involving both technical and conceptual characterisation. It is a fully automated process that is designed to allow future preservation processes to also be fully automated.

5.3.1. Technical characterisation

Technical characterisation involves discovering properties of the actual files with the aim to discover those properties that might determine whether the file is in an obsolete technology and thus in need of some form of preservation action:

- First of all it attempts to identify the format of each file using DROID [6]. Importantly, this links the file to a format identifier, which can be used to automate preservation policy decisions based on information stored in the Technical Registry.
- Format validation then takes place. The initial format identification determines the best validation tool to run (e.g., Jhove [7] is run for JPEG files). (The policy decision of which tool to use for which initial format identification is stored in a machine-readable way in the Technical Registry thus enabling this process to be automated). This can lead to the format identification result being updated. For example, DROID is currently unable to distinguish TIFF3, TIFF4, TIFF5 and TIFF6. However, Jhove is capable of validating each of these formats and will thus be able to reject three of the four initial identifications.
- Each file then has key properties extracted by means of a tool. The tool used and the properties extracted are again format dependent and are determined by the policy in the Technical Registry. Again, importantly, each property is linked to a Registry identifier so that any policies associated with that property can be automatically applied.
- Where possible, embedded objects are extracted from each file and these are characterised in turn. This is important because the embedded object may be obsolete even if the container file is not. (Once again the tool to use to perform this extraction is based on the format of the container file and is based on machine-readable policy stored in the Registry).

5.3.2. Conceptual characterisation

Conceptual characterisation determines the conceptual units called "components" that need to be preserved. These are not necessarily equivalent to files since, being conceptual, they are not technology-dependent. For example, one component might be a "web page" which, in current technology in 2010, is likely to consist of many files (HTML, CSS, GIF etc.) that combine to produce a conceptual entity that needs to be preserved. However, there is no guarantee that the physical structure will be identical in future generations of technology.

Once these have been identified the technology-independent properties of these components should be measured. These form the "significant properties" of the component that should be invariant in a good migration. A record will be well preserved if all its components, all their properties and all the relationships between these components are preserved.

In practice, of course, the conceptual properties need to be measured in the technology present in the SIP so component properties are closely linked to the technical properties measured for individual files (or an aggregation thereof). However, the distinction between them is important even if there is often a one-to-one correspondence between a file and a component in current technology: file properties are technology-dependent and thus needn't necessarily be preserved while component properties are technology-independent and thus should be preserved. This will be discussed more in the preservation section below.

5.3.3. Quality assurance revisited

In practice, there is an overlap between the steps involved in generating the AIP and performing quality assurance. For example, quality assurance restrictions on permitted formats or allowed properties of files (e.g., preventing encrypted PDFs from being ingested) can only be applied after technical characterisation has taken place. Also, some of the steps listed in section 5.2 (e.g., virus checking) lead to metadata (such as information on the virus checker used) being added to the AIP.

5.4. Generate Descriptive Information

Part of the OAIS ingest process requires the system to ensure that all the systems that need to hold descriptive information are synchronised. The Austrian State Archives maintain a catalogue that contains descriptive information about all of their holdings, whether this is on traditional media or electronic. Hence, it is necessary for DigLAimBund to be able to produce a snapshot of the descriptive information needed by a catalogue system and making it available to that system. This is done using OAI-PMH.

5.5. Coordinate updates

The last step of ingest defined in OAIS it to send the AIP to be stored in the combination of the relational database and the bulk-file storage system. This is described in more detail in the next two sections.

6. DigLAimBUND STORAGE

6.1. Receive and provide data

The bulk-storage system used in DigLAimBund is EMC Centera. SDB interfaces to such a bulk-storage system through a series of APIs that isolate changes in the storage system and changes in the repository software. There are interfaces to allow content to be stored and retrieved in a variety of ways (e.g., with or without a metadata snapshot, with content files stored independently or within a package, whether to sign a package or not etc.). Each of these decisions will be discussed in turn.

Metadata is stored in the database so, if this is properly backed up, storing a metadata snapshot may seem to be unnecessary. However, adding such a snapshot means that in the event of a non-recoverable database failure the storage system contains enough information to restore a record to a known state. On the other hand, it should be noted that the database contains the latest set of information about the record (e.g., information on access events) so some information will be lost if the database is lost. Of course, this information could be stored in the bulk storage system as well if the snapshots are refreshed at regular intervals but this would place quite a burden on the storage system. DigLAimBund has opted for a reasonable middle ground and does add a metadata snapshot to the storage system but will only update it if a preservation action occurs: not in the event of an access event or a descriptive metadata update. Note that any descriptive metadata updates will also be stored in the catalogue system so they are backed up independently anyway. This means that the historical information of who accessed the record when would be lost in the event of a non-recoverable database failure but this seems to be a reasonable compromise.

DigLAimBund also stores AIPs as packages (one AIP per SIP received). This is partly a policy decision and partly a consequence of the storage system which, if used to store a lot of small files (as might be the case when storing a web site), will waste a lot of expensive storage capacity.

Finally the packages are signed with a XadES signature, which is used to further guarantee the authenticity of the package.

6.2. Managing storage

OAIS requires the system to manage the storage hierarchy, replace media as required and provide disaster recovery. All of these features are provided through the standard features of EMC Centera.

6.3. Error checking

EMC Centera provides built-in features that check every file against its fixity values in order to pick up any corruption. In addition, SDB provides an on-going integrity checking function (based on a least recently checked algorithm) that does the same across as many storage adaptors as the system has (this allows for, for example, a second copy to be stored in different storage technology). A further advantage of this duplication is that the SDB check also provides a means for checking that the list of files held in the metadata database and those actually stored are identical (and that the fixity values stored in both sub-systems are also the same).

7. DigLAimBUND DATA MANAGEMENT

7.1. Receive database updates

Database updates (whether ingest requests or update requests for a variety of reasons described below) are received by the SDB database and processed by storing entities from the data model into appropriate database tables with all the information held in an XML fragment and some information denormalised into standard relational database fields where fast access or querying capability is required.

7.1.1. Post-ingest updates

SDB provides the ability for descriptive metadata to be enhanced. However, it is also possible for this metadata to be updated in the catalogue system. Hence, exchange of information between the systems (via OAI-PMH) is very important.

In addition, DigLAimBund supports a few specific scenarios:

- Allow records to be moved to a new collection.
- Allow records to be appraised after ingest and then, if necessary, to be exported (in EDIAKT form) for ingest to another system or to be deleted altogether.
- Allow records to be deleted as a result of a court order.

Appraisal and deletion actions occur via a “four eyes” principle (i.e. the workflow requires a supervisor to approve an initial assessment) while deletion via a court order (a very rare event) will occur via a careful operating procedure. In order to support this SDB also includes the ability to “soft delete” (i.e. to immediately prevent the record from being visible to ordinary users while the full workflow is enacted).

Finally, updates can occur as a result of preservation actions (see below) or re-characterisation (re-running characterisation to take advantages of better tools).

7.2. Perform queries

All database accesses utilise Hibernate [8] so that the system is not dependent on any particular database engine technology (although Oracle 11 is used). This means that all queries onto the system work using HQL rather than SQL. All queries needed for operation of the system in normal circumstances are already built-in to SDB.

Of course for efficient querying it is necessary to use appropriate indexing. Hence, in addition to standard relational database indexes, SDB uses the Solr [9] search engine to index the descriptive metadata held in XML fragments and to perform full text indexing of the (text-based) content files.

7.3. Generate report

Reporting can be made in two ways in DigLAimBund: internal SDB reporting using the open-source Jasper Reports tool (which requires some programming ability but allows reports to be embedded within the application) and an external reporting tool using the Pentaho reporting tool (which allows simple reports to be created in a less technical way). In either case full access to the entities held in the database is provided including the audit trail and the workflow history so that the full provenance of every entity can be reported upon.

7.4. Administer database

This uses standard database tools provided by Oracle.

8. DigLAimBUND ACCESS

8.1. Coordinate access activities

8.1.1. Query Requests

DigLAimBund provides the ability for users to:

- Browse a tectonic to find a record of interest
- Search for records by simple search (across all information held) and by advanced search (i.e. by choosing the appropriate fields). This includes the ability to search within the full text of documents. Each search identifies records that match the criteria order by relevance and (where full text searching has occurred) identifies the documents within that record responsible for the hit.

Access is only provided to records that are within the rights of the individual user to view. Once a user has found a record they can view all the metadata known about it (including its place in the tectonic and descriptive metadata). They can also see the list of files held together with (for common formats) a snapshot of the file.

For archival staff all the information held in the metadata store is available including:

- The list of possible manifestations available for download
- For each manifestation, the list of files and the list of components (identified in conceptual characterisation) that constitute it.
- For each file, all the technical metadata held
- The full audit trail for each entity held.

8.1.2. Orders

Authorised users can order content in two ways: an ad-hoc order (immediate download or rendering of a single selected file) or an event-based order for a record.

8.2. Generate DIP and deliver response

When an order is received, the appropriate content is retrieved from storage and a DIP is generated. This requires the appropriate files to be retrieved from storage, their integrity checked and then to package them up into a package (e.g., a ZIP file). This is then delivered to the end customer. For event-based orders, this can take place in a number of ways (e.g., via a download, by e-mail or placing the content in an pre-assigned location and informing the end user).

9. DigLAimBUND PRESERVATION

9.1. Preservation Planning in OAIS

Most of the preservation activities required in OAIS are to do with planning rather than performing preservation and are mainly activities requiring human judgement.

These are, of course, very important activities. However, one of SDB's (and thus DigLAimBund)'s main features is "Active Preservation" (an automated way of performing preservation). This is explained in this section.

9.2. Policy

The Technical Registry contains information about, amongst other things, formats (and format technical properties) and migration pathways. This allows policy to be set about what makes a file obsolete and what to do to migrate files to a new format. This can be either an absolute measure (e.g., a statement that any file in a given format is considered obsolete) or a risk-based measure (e.g., a series of a criteria that contribute towards risk and if, when taken together, pass a threshold, would make a file be considered obsolete). The Registry also allows policies to be set for different reasons (e.g., obsolescence of the preservation copy could follow a different policy than obsolescence of the presentation copy).

The Registry can be used in two ways: either by allowing policy approval so that the official policy governing one particular scenario is clear or by allowing manual intervention in the otherwise automated preservation workflows to pick the policy appropriate to the particular scenario. In reality a combination of these approaches is in use as best practice in this area is still in development.

9.3. Determining files and records at risk

The policy criteria that determine obsolescence are stored in a machine-readable way which means that they can be automatically compared to the technical characteristics derived during ingest (or a subsequent re-characterisation) in order to determine which files are in need of action. It is then possible to work out which manifestations of which records within the repository are in need of some form of preservation action. In order to identify which manifestations are relevant, each manifestation of a record is typed (e.g., "preservation" or "presentation").

This process can take place at any time so, in order to prevent repeated migrations, each manifestation is also assigned an active flag. This is set to ensure that there is only one active manifestation of each type allowed at any one point in time and only active manifestations of the type that corresponds to the migration reason (and thus to the stored policy) are considered for migration.

9.4. Extending to linked records

Having established which record manifestations need attention, the system then extends the migration to include all other records within the branch of the tectonic. This is since, for example, a parent record of a record in need of attention needs to be deliverable in full in the new manifestation. Hence, it is essential that the system checks that the new manifestation of the parent (which will include the files of the child record) is coherent. This may or may not lead to any additional file migrations but it will lead to additional verification checks if there are links between the records. As an example of this, the parent record could be a web site and the child record could be a report held within that web site. If the report were migrated from, say, Word to PDF leading to a change in file name extension, the html page of web site would need to be slightly altered in the new manifestation so that it links to the new file.

9.5. Migration

Having determined the extent of migration needed, the system then determines all of the components of the records discovered during conceptual characterisation (described above). Some of these components will contain files that need to be migrated (either because of obsolescence or because of the knock-on effects such as the web page described above). These are the atomic units of migration since these units and their appropriate properties and relationships are the things that are preserved during migration even though the physical structure of the files that manifest them may change.

Based on the policy described above, each such component runs through a migration pathway, which determines the migration tool(s) to use, thereby migrating the set of files it contains into a new set of files. The new files produced then run through technical characterisation and the new component manifestation through conceptual characterisation. This latter step identifies the new component manifestation's properties and relationships that should be identical to those in the original (subject to any tolerances permitted in the policy owing to, perhaps, acceptable rounding errors or an expected degradation such as a lower resolution image being created for preservation). All of this information is held in XML thereby again allowing this process to occur automatically.

Once this process has been completed successfully, the system can aggregate the component manifestations into record manifestations and ingest these into the repository. The system also ensures that the superseded manifestation is turned inactive so it is not migrated again.

9.6. Alternative approaches

As described above, SDB currently supports the case of "just in case" migration. However, "on demand" migration would be possible by adding an appropriate workflow. This could simply be access workflow (i.e. create the migrated copy and provide it to the end user) or could be a full preservation workflow using "Active Preservation" if the intention was to ingest the ne manifestation in addition to providing immediate access).

10. In addition, trial emulation functionality is currently being added to SDB as part of the EU-funded KEEP project [10].DigLAimBUND ADMINISTRATION

DigLAimBund includes sophisticated administration features to perform the features required by OAIS namely:

- Manage the system configuration. This includes performing standard IT system administration (e.g., monitor backups, database performance etc.).
- Establish standards and procedures by configuring the workflows for ingest, access, storage, data management and preservation. Workflows can be started manually, at regular intervals or in response to monitored events such as the arrival of a SIP in a specific location. If a step requires individual attention the appropriate user is informed via e-mail. Each user when they log-in can see a list of any actions awaiting their input. It is also possible to report on the progress of workflows or to

monitor what happened in workflows that have been completed at any time in the past.

- Control access rights
- Allow archival information updates (e.g., metadata editing, deletion and appraisal as described above)
- Audit information (e.g., to allow users to report on the contents of the archive or an authorised user to view the audit trail of any entity in the system).
- Negotiate submission agreements. Transfer agreements (including restrictions on SIP sizes, allowed formats etc.) can be set-up and automatically verified during ingest

11. CONCLUSION

The Austrian State has been investing heavily in electronic records management and archiving. This has already led to the use of records management within government agencies (via ELAK) and a system for transferring material between agencies (using EDIAKT).

It now also includes an archival system (DigLAimBund) that will be operational in late 2010.

Hence, much work has been done but it is anticipated that further work will be needed especially in the establishment of the best practice that is needed to run the system efficiently. In the interests of developing and sharing this, Tessella and institutions that utilise the SDB system have formed an SDB Users Group that has already met on four occasions to participate in this exchange of hands-on information.

12. REFERENCES

[1] Austrian State Archives, http://www.oesta.gv.at

[2] EDIAKT Viewer/Creator , http://www.ag.bka.gv.at/index.php/EDIAKT-Viewer

[3] Planets project home page, http://www.planets-project.eu

[4] Brown, A.: Automating preservation: New developments in the PRONOM service, RLG DigiNews 9(2) (2005)

[5] PRONOM home page, http://www.nationalarchives.gov.uk/pronom

[6] DROID home page, http://droid.sourceforge.net

[7] Jhove home page, http://hul.harvard.edu/jhove

[8] Hibernate home page, http://www.hibernate.org/

[9] Solr home page, http://lucene.apache.org/solr/features.html

[10] KEEP project home page, http://www.keep-project.eu/