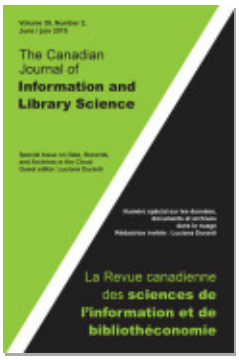
Archival Cloud Services: Portability, Continuity, and Sustainability Aspects of Long-term Preservation of Electronically Signed Records / Les services d'archivage dans un nuage informatique : Portabilité, continuité et durabilité: Aspects de la conservation à long terme des documents signés électroniquement



Hrvoje Stancic, Arian Rajh, Hrvoje Brzica

Canadian Journal of Information and Library Science, Volume 39, Number 2, June juin 2015, pp. 210-227 (Article)

Published by University of Toronto Press
DOI: *https://doi.org/10.1353/ils.2015.0012*

Archival Cloud Services: Portability, Continuity, and Sustainability Aspects of Long-term Preservation of Electronically Signed Records

Les services d'archivage dans un nuage informatique : Portabilité, continuité et durabilité : Aspects de la conservation à long terme des documents signés électroniquement

Hrvoje Stancic
Faculty of Humanities and Social Sciences, University of Zagreb
hstancic@ffzg.hr

Arian Rajh
Faculty of Humanities and Social Sciences, University of Zagreb
arian.rajh@halmed.hr

Hrvoje Brzica
Financial Agency, Croatia
Hrvoje.Brzica@fina.hr

Abstract: The authors discuss key processes needed to establish archival cloud services. This is done by examining long-term preservation mechanisms and their elements. In this context, the authors explore the electronic document safe concept and analyse two models of cloud-based digital archives. The authors propose a model of archival cloud services and discuss the portability, continuity, and sustainability aspects of long-term preservation of electronically signed records.

Keywords: archives in the cloud, electronic signatures, records portability, post-custodial paradigm, changing role of archives

Résumé : Les auteurs de cet article discutent des processus clés nécessaires à la mise en place de services d'archivage par nuage informatique. Pour ce faire, ils examinent les mécanismes de conservation à long terme et les éléments qui les composent. Dans ce contexte, ils explorent le concept de coffre de sûreté pour documents électroniques, et ils analysent deux modèles d'archives numériques basés sur un nuage informatique. Les auteurs proposent un modèle de services d'archivage par nuage informatique et discutent de la portabilité, de la continuité et de la durabilité en tant qu'aspects de la conservation à long terme des documents signés électroniquement.

Mots-clés : archives en nuage informatique, signatures électroniques, portabilité des documents, paradigme de post-surveillance, changement du rôle des archives

Introduction

Digital records are regularly stored in digital archives—solutions that could be made fairly safe in terms of long-term preservation if made compliant with the relevant standards. However, the increasing momentum of cloud storage might downgrade the level of overall quality of digital records preservation because it mainly focuses on the accessibility of the stored records. Digital records are being increasingly timestamped or signed by (advanced) electronic signatures, and (qualified) certificates are being associated with them. This adds complexity to the preservation of their authenticity, integrity, reliability, usability, and non-repudiation. The matter of legal jurisdiction over the records stored in the cloud creates additional uncertainty. What used to be a relatively controllable environment for digital archives has become volatile with the use of cloud services. Cloud service providers (CSPs), as new players, are being introduced into the archival process that used to involve only two parties—archives and record creators. In this new landscape, the role of archives changes. While the post-custodial paradigm has shifted the role of the archives from recordkeepers to supervisors of record creators, the introduction of cloud services might push this paradigm one step further. Archives should try to influence cloud-service providers to develop services more attuned to the archival standards, while, at the same time, counsel record creators in how to approach cloud services and set up or require proper archival processes.

The aim of this article is to analyse the relevant standards, explain the elements of a public key infrastructure (PKI) in the context of long-term preservation, briefly present the concepts behind cloud solutions, discuss archiving in the cloud as a process, examine the concept of electronic document safe in the context of trusted cloud service, analyse two models of cloud-based digital archives, and, finally, building on all of this, propose a model of archival cloud services supporting the long-term preservation of electronically signed records.

Relevant standards

The International Organization for Standardization (ISO) 15489 is a basic records management standard related to the establishment of the environment for records management in public and business organizations, records management policies, internal practices, systems, training, and other mechanisms. It also defines the expected qualities of records (for electronic records and information stored in document management systems, it is expanded in ISO 15801). Standards related to ISO 15489 lead practitioners to analyse their business processes and comprehend the business context before designing records management environments and systems (ISO 26122), to design relevant metadata schemas (ISO 23081), to assess related risks (ISO 18128), and to work adequately with digitized (ISO 13028) and digital records (ISO 16175, ISO 13008) in automated system surroundings (ISO 14641). ISO 17068 states what requirements have to be met in the third party repository. In addition, there are several ISO standards concerning information security, ISO 27001 being one of them. ISO

16363 specifies practices for assessing digital repositories and systems' trustworthiness, and ISO 16919 specifies requirements for certification bodies according to ISO 17021 and ISO 16363 criteria. ISO 14721 defines the reference model of archives—that is, the system or digital repository capable of long-term preservation of information, records, and digital objects. It defines a contemporary archival environment that consists of producers, archives (system, digital repository), management, and consumers. Furthermore, it defines the basic functional model of such a system with functional entities such as ingest, archival storage, data management, system administration, preservation planning, and access. Finally, it defines logical information models of information object and information packages (the submission information package delivered by the producer or client to the archives, the archival information package preserved in the system, and the dissemination information package prepared for further usage by the designated community).

PKI elements for long-term preservation of electronically signed records

The concept of long-term preservation of digital records requires a complex digital solution (Brzica, Herceg, and Stancic 2013). The terms electronic signature, digital certificate, non-repudiation, trusted archives service, timestamp and trusted digital timestamping will be explained. However, first, for a better understanding of these concepts, the concept of PKI needs to be explained.

PKI

A PKI represents a complex information infrastructure, which is used to manage electronic identities. PKI relies primarily on asymmetric encryption. Asymmetric encryption actually relies on a mathematically related pair of keys, one called the public key and another called a private key, which are generated to be used together. The private key is kept secret and used only by its owner, while the public key is made available to anyone who wants to use it (Jacobs et al. 2003, 330–31). Modern systems can easily use keys with a length of 2,048 characters, which are impossible to break even by today's supercomputers.

Electronic signature and advanced electronic signature

There are two types of electronic signatures—basic (usually referred to just as "electronic signature") and advanced (Brzica, Herceg, and Stancic 2013). The European Telecommunications Standards Institute defines electronic signature as,

> essentially the equivalent of a hand-written signature, with data in electronic form being attached to other electronic subject data (invoice, payment slip, contract, etc.) as a means of authentication. Electronic signature is not just a "picture" of the hand written signature. It is a digital signature that uses a cryptographic transformation of the data to allow the recipient of the data to prove the origin and integrity of the subject data. (*Electronic Signature* n.d.)

European legislation in EC Directive 1999/93 on a Community Framework for Electronic Signatures states that an electronic signature needs to meet the following requirements to become an advanced electronic signature:

a) it is uniquely linked to the signatory;
b) it is capable of identifying the signatory;
c) it is created using means that the signatory can maintain under his sole control; and
d) it is linked to the data to which it relates in such a manner that any subsequent change of the data are detectable.[1]

Digital certificate and qualified digital certificate

Digital certificates are digital records used to confirm the identity of a person, an organization or a machine. A digital certificate is valid for a certain period and contains several additional elements. EC Directive 1999/93 allows issuing of the so called qualified certificate, which is based on the RFC 3039 standard (Santesson 2001) and implements the concept of non-repudiation. Annex I of the Directive sets the requirements for the qualified certificate. It must in particular include:

1. an indication that the certificate is issued as a qualified certificate;
2. the identification of the certification-service-provider and the State in which it is established;
3. the name of the signatory or a pseudonym, which shall be identified as such;
4. provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
5. signature-verification data which correspond to signature-creation data under the control of the signatory;
6. an indication of the beginning and end of the period of validity of the certificate;
7. the identity code of the certificate;
8. the advanced electronic signature of the certification-service-provider issuing it;
9. limitations on the scope of use of the certificate, if applicable; and
10. limits on the value of transactions for which the certificate can be used, if applicable.

Timestamp and trusted digital timestamping

According to Carl Wallace, Ulrich Pordesch, and Ralf Brandner (2007, 5), a digital timestamp is an attestation generated by a time stamping authority (TSA)—a trusted service—that a data item existed at a certain time. Jasmin Ćosić and Miroslav Bača (2010, 1227–28) explain that

> time stamps are typically used for logging events, in which case each event in a log is marked with a time stamp. In file systems, time stamp may refer to the stored date/time of the file creation or modification. Trusted time stamping is the process of securely keeping track of the creation and modification time of a document. . . . Trusted TSA can be used to prove the consistency and integrity of digital evidence in every stage of its existence.

Formats of electronic signatures

In the earlier discussion, the technologies and concepts supporting trust in electronic records were explained. It was shown that the concept of an electronic signature can be viewed as the basis for developing all other technologies. Further, electronic signatures can be realized through several formats of electronic signatures—XML Digital Signature (XMLDSig), XML Advanced Electronic Signature (XAdES), Cryptographic Message Syntax Advanced Electronic Signature (CAdES), and PDF Advanced Electronic Signature (PAdES) (Brzica, Herceg, and Stancic 2013).

Cloud services

Cloud solutions, in general, can be deployed in various forms, such as the public cloud, which can used by anyone, the private cloud for private use by a single organization, the community cloud for a group of users, or the hybrid cloud. Users of cloud solutions are offered software or applications, platform or entire environments, as well as infrastructure or entire virtual datacentres (Stancic, Rajh, and Milosevic 2012). Whether to develop a cloud-hosted system or a system on premise depends on the complexity of an organization's information technology (IT) environment, needed functionality, size of the organization, data volume, legal regulations, IT skills of the in-house experts, resources, as well as operational costs (*Cloud: On-Premise or Hybrid?* n.d.): "Applications and services need to be run where they are most efficient and not just because cost is the most attractive option. In the long-term, falling into the 'all Cloud' solution trap can prove to be more expensive, time-consuming and problematic" (*On-Premise versus Cloud-based Solutions* 2010).

Archiving in the cloud as a process

As Sue McKemmish (2013, 19) has explained,

> cloud computing offers attractive benefits including significant cost savings, efficiencies, flexibility and scalability, as well as opportunities for the innovative development and delivery of new services. It also carries significant risks associated with the security, privacy, integrity, authenticity, accessibility and digital continuity of data and records in the cloud. There are also issues relating to commercial continuity and the lack of transparency of cloud services that impact on recordkeeping and archiving.

All this raises a question of entrusting records to the cloud. To minimise risks and maximise benefits a standardised process of archiving in the cloud should be used.

A generic business process of archiving in a cloud environment should include a creator's part and a CSP's part (see Figure 1). The creator creates documents in sustainable formats and signs them electronically (1). Verification data should be preserved for later use (2). Before submitting documents to the chosen service provider, documents and signatures should be checked (3), and documents should be declared as records (4). Then the service provider ingests records (5) and processes them (6). All documents could be verified with qualified eStamp mechanism (8). Archiving should be done by creating a copy in a

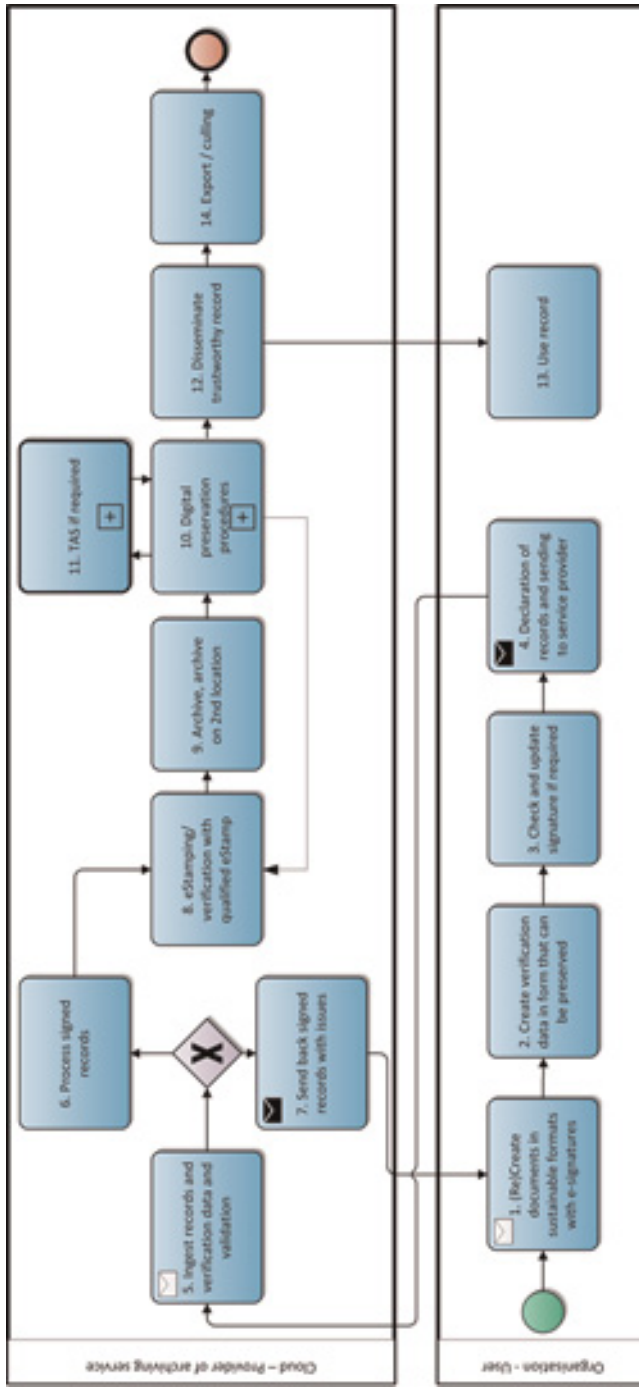


Figure 1: Generic business process of archiving in cloud environment

secondary location (9). Digital preservation procedures (10) should include file format migration, if needed. The service provider should have implemented a procedure of regular validation of signed records with a trusted archives service (TAS) emulator (11). The TAS process is treated as specific sub-process with its own mechanisms (for example, eStamping). A record is provided (12) on demand to the creator who uses it (13). The service provider should actively promote long-term preservation measures to the creator and communicate with the creator when verification/validation criteria are not met.

Jos Dumortier and Sofie Van den Eynde (n.d., 7) explain that

> a TAS must guarantee that it will still be possible to validate an archived document years after the initial archival date, even if the applications that have been used at signature creation time are no longer in use. In other words, the TAS should maintain a set of applications (viewers as well as signature validation applications) together with the corresponding platforms (hardware, operating systems) or at least an emulator of such applications and/or environment in order to guarantee that the signature of the document can still be validated years later.

Trusted cloud service: underlying concept

To better understand the complexity of building a trusted cloud service, the underlying concept of the electronic document safe (EDS) needs to be analysed. An explanation of the concept in the context of secure storage of officially issued governmental documents will show how the authenticity of digitally signed documents and their trustworthiness can be preserved over the long term.

EDS

In the context of cloud services, Peter Deussen and his colleagues (2012) define the concept of the EDS as a secure storage for official documents (for example, used as a part of citizen support services). The EDS functionalities are secure long-term storage of official electronic documents and established electronic workflows among administration, enterprises, and citizens. Employees of government agencies can store documents in the EDS of any user. On their part, users can access only their own EDS, and, for doing so, they need a special application providing secure encrypted communication and authentication. The Fraunhofer Institute has developed a version of the EDS called eSafe. It shares with the EDS the idea that documents should be stored in a trustworthy, secure way within a cloud infrastructure, but it goes further by describing a mechanism to fragment and distribute such documents among several cloud storage providers, thus making it very difficult for an unauthorized person to retrieve the original document (Breitenstrom, Brunzel, and Klessmann 2008).

Regarding the feasibility of developing EDS solutions, there are at least two hypothetical issues that need to be addressed: privacy protection and long-term service availability. Christian Breitenstrom, Marco Brunzel, and Jens Klessmann discuss the data protection issue in the context of privacy protection by analysing the requirements of storing personal data in public cloud infrastructures and using those data to interact with public sector authorities. Significantly, when an EDS

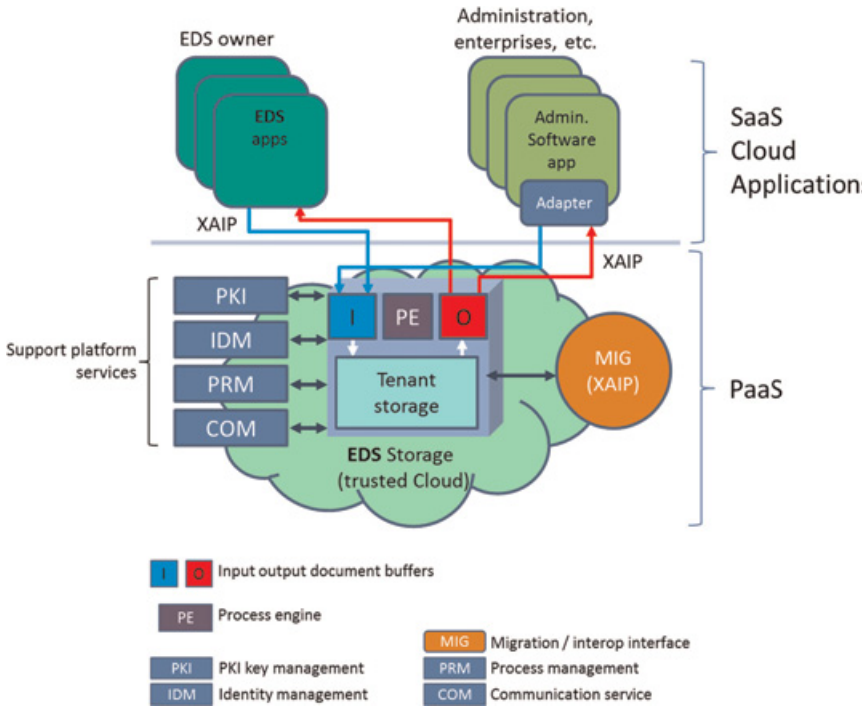


Figure 2: EDS principle architecture (Deussen et al. 2012, 45)

is established, citizens can approve that personal data are stored and processed electronically. Hence, data privacy applies only insofar as citizens have to trust the EDS provider. Since data in the EDS are encrypted and thus not visible to the provider, the "data protection barrier" can be considered to be low and the principle applied can be qualified as data anonymization.

Second, if we look at the EDS as a technical solution for supporting administrative processes, then the government agencies should guarantee and take responsibility to ensure the continuous availability of the service. For some types of records, it could be more than 100 years. Therefore, the most important question is how a private sector provider is capable of giving sufficient guarantees on its own continued existence, future business orientation, and so on. A possible solution is to maintain a governmental cloud provider as a fall-back (or business continuity) solution, while allowing public sector providers to participate in the emerging market of electronic document and records storage (Deussen et al. 2012, 43–44). Of course, to achieve this, political and budget-related decisions need to be made first. The infrastructure that needs to be developed to establish an EDS solution in the cloud is shown in Figure 2.

The main component of the EDS system is the EDS storage—that is, a cloud-based infrastructure providing storage, access, and management functions. It comprises a tenant storage containing the documents of the EDS user and

several components to handle access, authorization, and usage. Input (I) and output (O) components are responsible for managing storage of the documents requiring authorization to be ingested into an EDS or delivered to the users, while a process engine (PE) is responsible for the coordination of the actual usage. The document representation format used in the EDS is the XML-formatted Archival Information Package (XAIP). Long-term preservation data formats such as XAIP or the universal object format (UOF) usually contain a combination of data and metadata. For example, XAIP was designed for an archives system, and its structure is based on the technical directive of the Federal Office for Information Security (Preservation of Evidence of Cryptographically Signed Documents 2011).

The archival information package is an XML file that contains the data and the corresponding metadata, while the UOF stores the data and metadata, based on the Metadata Encoding and Transmission Standard, in two separate files (Potthoff, Walk, and Rieger 2013, 28). Concretely, XAIP is structured in four parts: (1) archival package header that contains information about XAIP's logical structure; (2) meta information with the description of the transactional and archiving context of the content data; (3) content data that contains encrypted documents; and (4) certificate section containing digital signatures, digital certificates, information needed to verify digital signatures, as well as digital timestamps. Thus, the last part of the XAIP structure provides the relevant information on authenticity, integrity, and trustworthiness of the archived data objects.

Document migration

In the case that, during long-term preservation, a CSP providing EDS goes out of business, the records should be transferred to another CSP providing EDS. That is why the EDS architecture has the migration interface. Since the preserved materials contain records to be used as evidence and, thus, need to be signed to ensure authenticity, migration from one EDS provider to another has to be compliant with the laws and regulations governing the authorities who have initially issued these documents and are responsible for further processing (Deussen et al. 2012, 82). The process of migration of archival objects identified by their identifier (that is, the archive object identifier or AOID) from EDS 1's tenant storage (CSP A) to EDS 2's tenant storage (CSP B) is shown in Figure 3. To achieve this, certification service, signature validation service, and encryption service are needed. In addition, any transmission protocol supporting data encryption can be used for the migration of XAIPs.

Two models of cloud-based digital archives

A model of archival cloud services supporting long-term preservation proposed later on in this article is based on two models developed in Germany and Lithuania.

Germany: Federal Office for Information Security

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik [BSI]) developed a model of long-term preservation

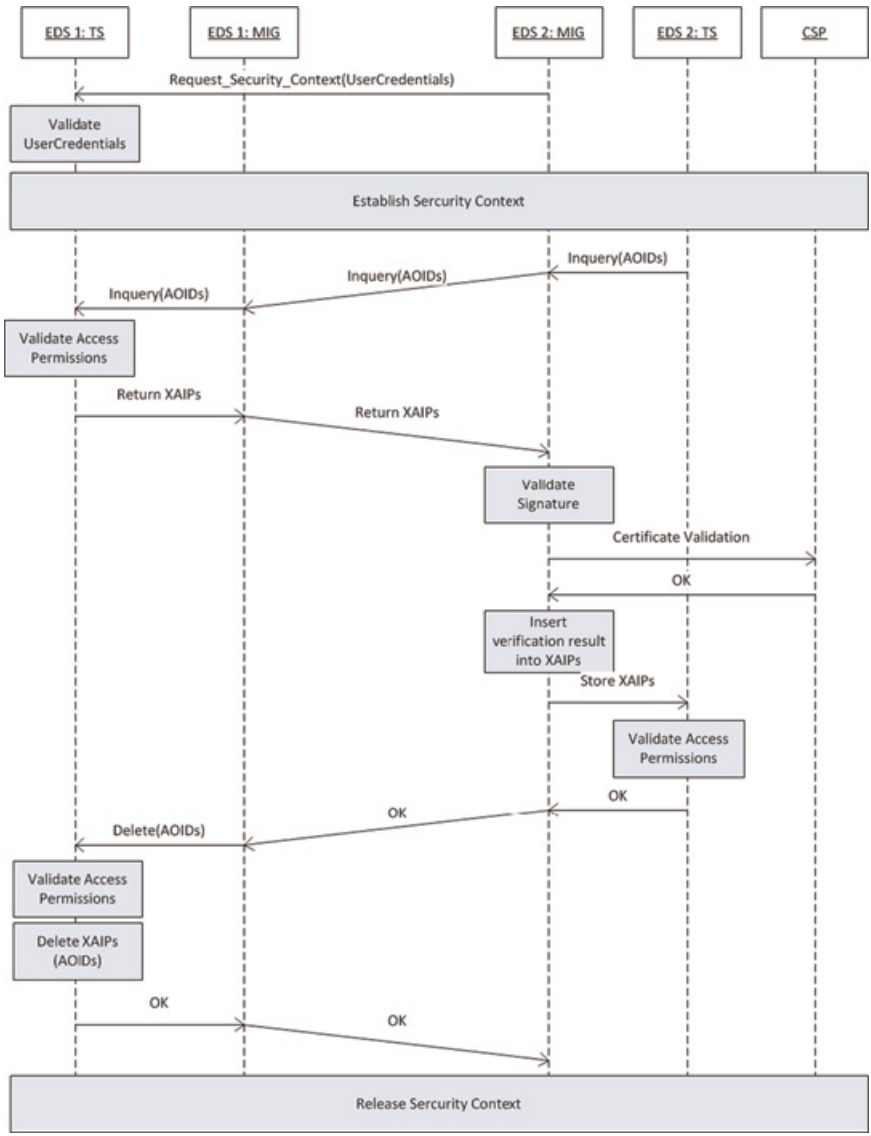


Figure 3: Document migration from EDS 1 (Provider A) to EDS 2 (Provider B) (Deussen et al. 2012, 84)

of digitally signed documents based on several ISO standards and the German Federal Archiving Act (Bundesarchivgesetz).[2] BSI has published technical guidelines explaining the architecture of the system responsible for long-term preservation—BSI Technical Guideline 03125 on the Preservation of Evidence of Cryptographically Signed Documents (BSI Guidelines) (Federal Office for Information Security 2011).

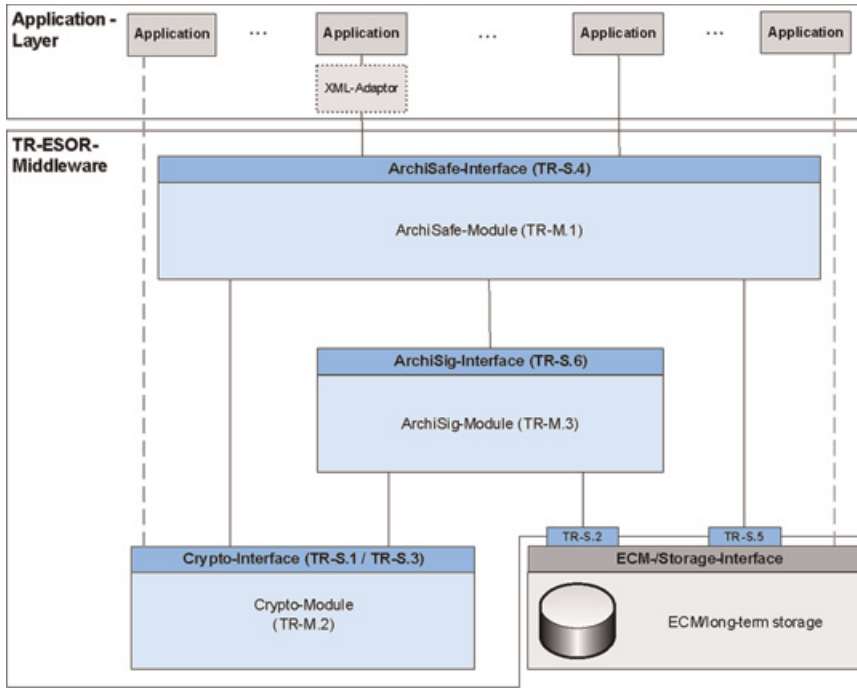


Figure 4: BSI referent architecture (Federal Office for Information Security 2011, 41)

BSI architecture comprises two main parts: (1) IT infrastructure for long-term storage and (2) IT applications archiving data and documents or working with them. The IT infrastructure used for archiving typically consists of:

- an enterprise content management / long-term storage system that includes and manages various storage media used for archiving and that guarantees the reliable and secure access to the storage media for the deposit, retrieval, and deletion of archived documents and data and
- the middleware, including the cryptographic components that support the preservation of the elements required by the laws of evidence governing the archived documents (and data). (Federal Office for Information Security 2011, 15–16) (see Figure 4).

Lithuania: electronic archives information system

The first Lithuanian system for working with electronic signatures was the e-Servicing System of the Insurers (EDAS), launched in 2007 by the State Social Insurance Fund Board of Lithuania. The EDAS system uses XAdES format of electronic signatures to sign the documents. Although metadata could be signed separately, as a sub-tree within the XML metadata file, the basic principle of the Lithuanian approach is that the metadata are integral part of the electronic document.

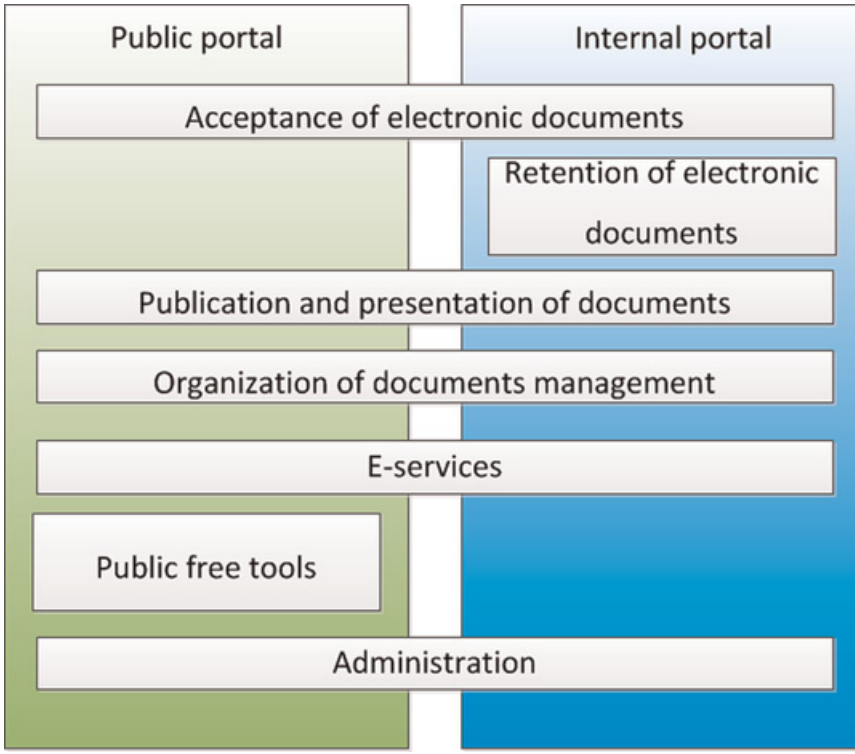


Figure 5: Modules of EAIS (Ragaisis et al. 2012)

A further step was to develop the Electronic Archives Information System (Elektroninio archyvo informacinė sistema [EAIS]) in 2011 as the final step in the Lithuanian government's preparation to fully work with e-documents (Elektroninio archyvo informacinė sistema 2011). EAIS enables archiving of the official e-documents signed with advanced electronic signature. The system ensures integrity, authenticity, non-repudiation, and usage during long-term preservation. The EAIS architecture consists of a public portal, an internal portal, and the storage of electronic documents. Storage is done in two geographically remote electronic archive data centres. Modules of public and internal portals are shown in Figure 5.

A model of archival cloud services supporting long-term preservation

The model of archival cloud services supporting long-term preservation proposed here builds upon the previously explained concept of electronic document safe and the two implementation models, taking into account the specifics of electronically signed records and archiving in the cloud environment as a business process.

System functionality

An archival cloud service supporting the long-term preservation of electronically signed records should preserve the integrity, authenticity, and confidentiality of stored records. It should make records available and usable—that is, maintain their readability. Data protection and system security should be enforced. At the same time, an archival cloud service should be expected to provide functionalities such as document creation, e-signing, archiving of non-signed and signed documents and records, records publication (with visualization of electronic signature), indexing, search and retrieval of archived records, provision of proof of evidence, preservation procedures not influencing the evidential capacity of preserved records, deletion of records, and administration.

There could be at least two expected access points to such an archival cloud service: one internal, used by governmental bodies as the creators of documents and records, and one external, used by citizens accessing the records. The Lithuanian experience with the EAIS system shows that the users would accept such a system if free software tools were offered—for example, for document preparation, e-signing, viewing, and verification of official digital documents. Those tools could be offered either as desktop applications having connectors to the cloud service or as web applications (software-as-a-service [SaaS] approach).

Automated processes, such as those for the digitization of documents to be stored in PDF/A format or those for embedding electronic signatures in the PDF/A documents, could be added to the system. An example of such an addition can be found in the e-health domain when medical documentation, such as x-ray images, need to be scanned and archived.

Key processes

To implement the system of archival cloud services supporting long-term preservation, it is necessary for the following to happen:

1. Electronic signature and timestamp should be created, verified, renewed, and stored in a safe and trustworthy way that is compliant with the relevant legal framework.
2. Data needed for later verification of electronic signature should be obtained immediately after its creation and/or verification. The verification data should be ingested along with the records.
3. All verification steps and results of the verifications should be logged and stored in the format that would guarantee non-repudiation.
4. Electronic signatures should be renewed before the expiration of the protection measures used in cryptographic algorithms. The renewal should be done according to the legal regulations and by a (semi-)automatic and economic process.
5. As a result of technological advancements, which have caused cryptographic algorithms considered strong today to be weak in the future, digital timestamps should be added. This way, to resign electronically signed records, it would be sufficient to certify them with a qualified timestamp, which consists of at least one qualified electronic signature.

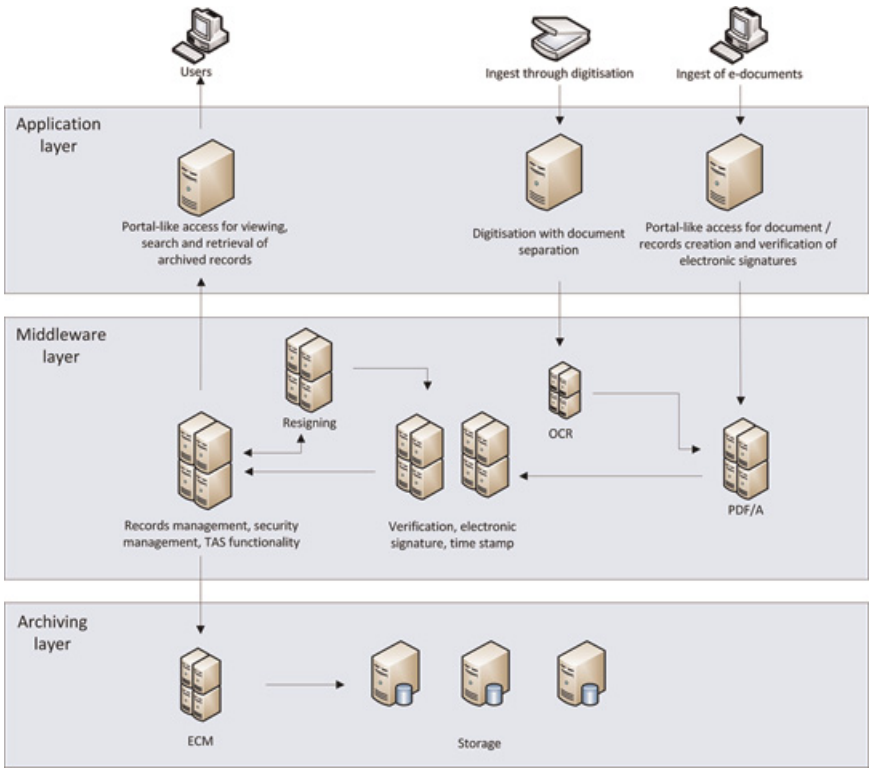


Figure 6: Architecture of archival cloud services supporting long-term preservation

6. The system components used for access to the content of the preserved records should be able to visualize electronic signatures, certificates, and the results of their verification.
7. The integrity of the non-signed records being submitted for long-term preservation need to be secured by cryptographic methods, such as hash values or electronic signatures and qualified timestamps.
8. The system should be, at a minimum, located at two geographically distant locations in case of data replication and disaster recovery situations.
9. The system should implement a trusted archives service) process—that is, ensure the processes of validation of archived, electronically signed records, years after ingest in the archives, in spite of the fact that the application solution for e-signatures and digital timestamping will be obsolete at that time.

System architecture

The architecture of the system of archival cloud services supporting long-term preservation should consist of at least three main layers: (1) application layer; (2) middleware layer; and (3) archiving layer (see Figure 6).

1. The Application layer accommodates web or portal as well as desktop applications. The applications should be used for creating documents that will be archived in the formats compliant to the standardized long-term preservation formats (for example, PDF/A of XML). They should also enable the functionality of electronic signature verification. To enable signature validation over the long-term preservation, it is suggested that the verification data of the electronic signature validity be archived—that is, proof of evidence, along with the signature—that is, with the e-signed document/record. The applications should also be used as trusted viewers. Trusted viewers are used for viewing electronically signed records, and they function as trustworthy components of the applications through which an advanced electronic signature is shown. An application layer should be used as interface, and it should provide functionalities for archiving records and enable search and retrieval of archived records and archived proof of evidence.
2. The middleware layer is a standardized and secure gateway that controls the access of applications to the archival storage. This layer logically separates applications in the application layer from long-term preservation storage. All actions, such as write, change, or delete, should be done through this layer. It is responsible for the cryptographic functions needed for preservation of evidence, such as creation of electronic signature, its verification, verification of electronically signed archival information packages, certificate validation, calculation of hash values, as well as request and verification of qualified timestamps. TAS functionality enables storage of software emulators used for verification and viewing of electronically signed records created by obsolete software. The functionality of resigning of electronically signed records can be used instead of the TAS functionality, since it enables resigning of the records using the latest signature formats. The process of resigning should be automated as much as possible.
3. The archiving layer is the layer used for long-term storage of archived records. It comprises main storage and remote storage. The technical principles of cloud storage physical organization apply here.

Discussion

The idea of an archival cloud service is very appealing due to the fact that creators of records are usually non-archival institutions that may lack infrastructure, technical capacities, and staff knowledge adequate for long-term preservation of electronically signed records. Although appealing, it is also challenging due to archival legislation, the protection of information, and the protection of national interests. As McKemmish states (2013), national legislation can be expanded to service providers regardless of the fact that the clients can be residents of other countries or in some cases even regardless of the location of data centres. It becomes more common today to use the data centres located in the creator's country so that the national legislation can be applied. Service providers may be asked to guarantee compliance with the corresponding creator's legal context.

There are four important aspects that should be considered when a creator decides to archive its holdings in the cloud: holding portability, digital continuity, environment sustainability, and warranty of compliance with corresponding legal context. Portability in this context has two meanings. First, it denotes an ability to transfer electronically signed records from a creator to the CSP's environment, during the ingest procedures, without losing reliability, authenticity, and trust in records. Suggested mechanisms include validation and verification procedures, checking file formats and so on. This aspect is not present if the creator is using CSP's SaaS concept for the creation of documents and records as an addition to, or part of, the archive-as-a-service concept because the records are already being created in the cloud.

Second, portability refers to the possibility of transferring creator's records from one CSP to another one—for example, if a CSP goes out of business, also without losing reliability, authenticity, and trust in records. Digital continuity refers to archiving electronically signed records and ensuring their usability in the time frame of their retention period and according to the business needs of the client organization (What Is Digital Continuity? n.d.; National Archives of Australia 2015). One of the available measures for ensuring digital continuity is the TAS function provided by the CSP. It should be kept in mind that the portability concept is inherent to the digital continuity concept.

Sustainability is a quality of the whole CSP's environment, and it can be ensured by technological and financial capacities and measures implemented by the CSP and assessed by the creator. For example, technology that is used for implementing a solution can be obsolescence resistant and based on well-known and robust solutions, the third-party provider can ensure adequate number of full-time employed technical support and administrative staff members, and the creator can check CSP's financial stability. Finally, for the protection of the information contained in records and their evidential capacity, the creator may consider asking CSP to store records within the creator's national boundaries.

Conclusion

The concepts of portability, continuity, and sustainability are preconditions for long-term preservation of electronically signed records by an archival cloud service at times when corresponding legal frameworks are not fully established everywhere. Achieving portability, continuity, and sustainability can stimulate a creator's trust in a CSP and, consequently, a creator's trust in its own archived records. Public trust in a records creator can ultimately depend on meeting these requirements. Portability is crucial for the successful transfer of files into a new CSP's environment, while sustainability ensures that this environment is stable. Continuity ensures maintenance of records between import and dissemination points. Stability of environment and service is twofold—it presumes technical excellence and response to changes in environment as well as financial stability of the CSP. Continuity and the technological part of the aspect of stability can be seen as further elaboration of the OAIS reference model's preservation planning function. They are conceptually similar to the preservation planning

function, but continuity is at the level of information and records and stability is above this level and expands on the capability of a system to preserve information and records according to the built-in mechanisms and methods. An example of meeting the continuity requirement is implementation of a proposal for conversion of a file format to an upgraded format submitted to the client by the CSP. An example of meeting the technological stability aspect can be switching from one conversion tool to another if the target file format is upgraded and the older conversion tool cannot do the job right. All of these criteria are not easy to define in the tendering procedures and contracts with CSPs, but information package prototypes testing in the first period of the execution of the contract, as well as periodical testing and testing after technological changes that may influence digital archival holding, can be foreseen and prescribed in such contracts. The models explained in this article, their underlying principles, and the proposed model of archival cloud services supporting long-term preservation could be used either as guidelines for choosing an archival CSP or for establishing such a cloud service.

Acknowledgements

This research was completed in the context of the international multidisciplinary research project InterPARES Trust, http://www.interparestrust.org.

Notes

1. EC Directive 1999/93 on a Community Framework for Electronic Signatures, [2000] OJ L13.
2. Bundesarchivgesetz, 1988, http://www.bundesarchiv.de/bundesarchiv/rechtsgrundlagen/bundesarchivgesetz/index.html.en.

References

Breitenstrom, Christian, Marco Brunzel, and Jens Klessmann. 2008. *White Paper: Elektronische Safes für Daten und Documente*. Berlin: Fraunhofer Institut für Offene Kommunikationssysteme. http://wwwold.fokus.fraunhofer.de/de/elan/_docs/_hpp-gruppe/esafe_white-paper_081219.pdf.

Brzica, Hrvoje, Boris Herceg, and Hrvoje Stancic. 2013. ''Long-term Preservation of Validity of Electronically Signed Records.'' In *INFuture2013: Information Governance. Zagreb: Deaprtment of Information and Communication Sciences*, ed. Anne Gilliland, Sue McKemmish, Hrvoje Stancic, Sanja Seljan, and Jadranka Lasic-Lazic, 147–58. Zagreb: University of Zagreb, Faculty of Humanities and Social Sciences.

Cloud: On-Premise or Hybrid? n.d. Bluesource Information Limited. https://d3759s1c6gf66q.cloudfront.net/u/_201211/52981741/59991441/dtwRJfTb/CloudOn-premiseorHybrid.pdf

Ćosić, Jasmin, and Miroslav Bača. 2010. ''(Im)Proving Chain of Custody and Digital Evidence Integ-rity with Time Stamp.'' MIPRO: *Proceedings of the 33rd International Convention*, 1226–30.

Deussen, Peter, Klaus-Peter Eckert, Linda Strick, and Dorota Witaszek. 2012. *Cloud Concepts for the Public Sector in Germany: Use Cases*. Berlin: FOKUS Fraunhofer Institute for Open Communication Systems.

Dumortier, Jos, and Sofie Van den Eynde. n.d. *Electronic Signatures and Trusted Archival Services.*

Electronic Signature. n.d. http://www.etsi.org/technologies-clusters/technologies/security/electronic-signature.

Elektroninio archyvo informacinė sistema. 2011. http://eais-pub.archyvai.lt/eais/.

Federal Office for Information Security. 2011. *BSI Technical Guideline 03125 on the Preservation of Evidence of Cryptographically Signed Documents*. Bonn: Federal Office for Information Security.

Jacobs, J., L. Clemmer, M. Dalton, R. Rogers, and J. Posluns. 2003. *SSCP Study Guide*. Sebastopol, CA: Syngress Publishing.

McKemmish, Sue. 2013. ''Recordkeeping and Archiving in the Cloud. Is There a Silver Lining?'' In *Information Governance*, ed. Anne Gilliland, Sue McKemmish, Hrvoje Stancic, Sanja Seljan, and Jadranka Lasic-Lazic, 17–29. Zagreb: University of Zagreb, Faculty of Humanities and Social Sciences, Department of Information Sciences.

National Archives of Australia. 2015. *What Is Digital Continuity*?

On-Premise versus Cloud-based Solutions, White Paper. 2010. GFI Software.

Potthoff, Jan, Marius Walk, and Sebastian Rieger. 2013. ''Data Management According to the Good Scientific Practice.'' In *The Fifth International Conference on Advances in Databases, Knowledge, and Data Applications*, 27–32.

Ragaisis, Saulius, Adomas Birstunas, Antanas Mitasiunas, and Arunas Stockus. 2012. ''Electronic Archive Information System.'' In *Databases and Information Systems: Tenth International Baltic Conference on Databases and Information Systems—Local Proceedings, Materials of Doctoral Consortium*, ed. Albertas Čaplinskas, Dzemyda Gintautas, Audronė Lupeikienė, and Olegas Vasilecas, 107–14. Vilnius: Zara.

Santesson, S., W. Polk, P. Barzin, and M. Nystrom. 2001. *Public Key Infrastructure: Qualified Certificates Profile*, Internet X:509. Internet Society, 1–35. http://www.internetsociety.org.

Stancic, Hrvoje, Arian Rajh, and Ivor Milosevic. 2012. ''Archiving-as-a-Service: Influence of Cloud Computing on the Archival Theory and Practic.'' In *The Memory of the World in the Digital Age: Digitization and Preservation*, ed. Luciana Duranti and Elizabeth Shaffer, 108–25. Vancouver: UNESCO.

Wallace, C., U. Pordesch, and R. Brandner. 2007. *Long-Term Archive Service Requirements*. IETF Trust. http://dx.doi.org/10.17487/rfc4810.