Standards for the Preservation of Evidence and Trust for Electronic Records

Steffen Schwalm; BearingPoint GmbH; 10719 Berlin, Germany, Ulrike Korte; Federal Office for Information Security (BSI); 53175 Bonn, Germany, Detlef Hühnlein; ecsec GmbH; 96247 Michelau, Germany

Abstract

Information technology provides the elementary basis for efficient business processes in administration, business and science. Especially important is the preservation of the integrity and authenticity of digital records to maintain the conclusiveness of the documents supporting legal claims of the issuer or third parties and the proof of their correctness in electronic legal and business transactions. To achieve these aims it is required to preserve the evidence of the electronic records. Against this background organizational guidelines and technical mechanisms have been developed and standardized which enable public administrations and private enterprises to preserve the evidence and trustworthiness of their business records over a long period of time. The present contribution provides an overview of the existing and forthcoming standards in this area.

The use of the information technology for electronic business processes is established in public administration and private companies. Business records increasingly exist in different digital forms and systems. At the same time national and international laws and regulations for the compliance of business processes and electronic records have to be achieved by the using organization. This means that electronic records have to provide their authenticity, integrity, reliability and usability to act as an evidence of the business transaction in which they were developed [17-18]. This is the basis to make the transaction evident against third parties like justice or monitoring organizations. Against the background of retention periods between 2 and 100 years and the increasing innovation speed of information technology it is a special challenge to preserve the evidence of digital records to support legal claims and to fulfill the requirements mentioned above.

To be conform with these requirements it is necessary to know and use established national and international standards for records managements and the preservation of evidence of digital records in combination with standards for digital preservation.

Against the background of existing standards and currently ongoing standardization initiatives on an international, European and national level, the present contribution covers standards for trustworthy management and archival of electronic records and the preservation of evidence for cryptographically signed documents.

This includes on the one hand standards for the trustworthy archival and preservation of electronic documents and records such as ISO 14721 (OAIS) [13], DIN 31644 (Trustworthy Digital Archives) [1], DIN 31647 (Preservation of Evidence of Electronic Records) [3] and on the other hand standards for electronic signatures such as ISO 14533 ({C,X}AdES) [11-12], prEN 319 122 (CAdES) [4], prEN 319 132 (XAdES) [5], related policy requirements (prEN 319 521) [6], formats for Evidence Records (RFC 4998 [9] and RFC 6283 [10]) and further recommendations for the trustworthy preservation of evidence as laid down in TR-03125 (Preservation of Evidence of Cryptographically Signed Documents) [8]

The present contribution provides an overview about standards and procedures for the preservation of evidence and the trustworthiness of digital records by using cryptographic mechanisms, such as electronic signatures, time stamps and evidence records.

The description will also include practical guidelines to improve and implement legally viable electronic business processes, policies and IT-services for trustworthy and evidence preserving digital records. These guidelines include the integration of special requirements concerning trustworthy and sustainable e-government in the context of records management (e.g. ISO 15489 [14-15], ISO 30301 [17]) and digital preservation (e.g. ISO 14721 [13]) in Germany, Europe and beyond.

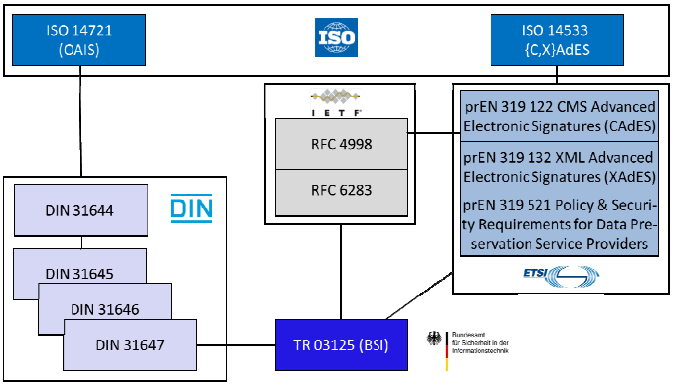

Figure 1. *Overview of the national, European and international Standards concerning trustworthy digital preservation*

ISO 30300, 30301 and 15489 (draft)

The ISO 303xx-standard-family provides a governance framework for the management of electronic records in public and private organizations. Based on corresponding fundamentals and a binding vocabulary it contains requirements and guidelines for the top management to implement and develop a management system of records (MSR) to achieve business regulations and stakeholder needs. For professionals the framework is completed by related international standards and technical reports, which provide the practical implementations of an MSR in an organization

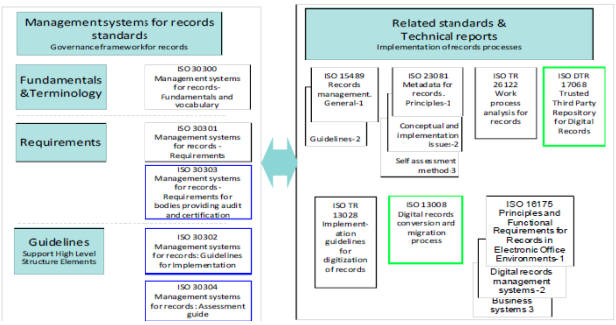

***Figure 2**. Overview of Management Systems for Records Standards [16-17]*

An MSR provides the organization to establish a systematic creation, usage and storage of electronic records based on mandatory rules and aimed at the stakeholder needs. Compliant records constitute the knowledge for business transactions, risk management or strategic decisions and therefore provide the foundation of a successful organization. Fundamental requirements of a compliant MSR are to ensure that authentic, unaltered (only allowed alteration is provided), reliable and usable information is created and managed to provide evidence for business transactions. Authenticity means in this context making evident who has created or sent a record. Reliability means that a third party will trust that the records were actually developed in the process with the shown content as it seems to be. Usability means that it is possible to use the content of the record in the necessary way.

A special need concerning the retention times of electronic records is the commitment to preserve the records providing the requirements as long as they are needed for the defined purposes governed by legal or business requirements. In short words: The MSR is an organizational system which is running based on mandatory rules, responsibilities and up-to-date information technology.

In order to meet the requirements for records management according to ISO 30300 [16], 30301 [17] and 15489 (draft) [15] the MSR has to ensure a reliable, secure, compliant, comprehensive and systematic records management. This includes special procedures to protect records against unauthorized alteration and to ensure that they can be used to verify their correctness with regular needs. This means that a compliant MSR will include organizational and technical methods to preserve evidence according to legal requirements [16-17] Records management is one of the main subjects, especially in e-government, where it is obligatory by law for compliant public administrations. It is also needed for business efficiency in private companies. These general standards like ISO 303xx and ISO 15489 (draft) are completed by technical standards for particular issues such as digital preservation, trustworthiness and the preservation of evidence of electronic records as discussed below.

ISO 14721

The Open Archival Information System standardized in ISO 14721:2012 [13] describes the basic functions or processes and information packages for digital preservation. A system according to OAIS is independent of the specific techniques of a specific product. This means that an Archival Information Package (AIP) which is stored in a digital archive is self-contained such that it includes all needed information such as content, metadata and other data to provide the purposes for which it was created (e.g. legal requirements, documentation requirements, compliance rules, stakeholder needs). In the context of records management it is often required that it is possible to prove the correctness of records against third parties e.g. using digital signatures or evidence records. The usage of OAIS may be seen as a fundamental necessity to preserve digital information such as electronic records.

DIN 31644

Based on OAIS and the various international experiences and discussions the German standard DIN 31644 [1] defines requirements for trustworthy digital archives. By means of a binding vocabulary, basic guidelines for the implementation and principles of trustworthy digital archives ("digitales Langzeitarchiv", dLZA) DIN 31644 contains a catalogue of organizational, functional and technical requirements concerning a dLZA. In this context a dLZA consists of persons (with defined roles and responsibilities) and technical systems (with defined and documented functions).

Like ISO 303xx DIN 31644 specifies that the purposes of the dLZA have to be defined to make it possible to be compliant to legal or contract based requirements. It means that if a dLZA is used to preserve electronic records it has to include processes, responsibilities and functions to provide the basic conditions for records management given in ISO 30xx and related standards. The dLZA has to define the significant properties for the information packages referred to OAIS (for example SIP, AIP and DIP) including rules for the relevant functions ingest, archival storage and access to prevent unauthorized usage and alteration. According to the specific use cases the concrete implementations may be different, e.g. historical archives (preservation for historians), public administrations or private companies (preservation for legal and business needs) [1-2].

DIN 31647 (draft)

The German standard DIN 31647 (draft) [3] verbalizes functional and technical requirements on a system for the preservation of evidence of cryptographically signed electronic records. Cryptographically signed means all electronic records which authenticity and integrity is protected by crypthographic methods such as digital signatures and timestamps and which digital evidence should be preserved. The standard completes a DIN 31644-corresponding trustworthy digital archive with the needed functions for the preservation of evidence of the stored records. This particularly includes the preservation of the authenticity, integrity and reliability of the electronic records. In these requirements DIN 31647 (draft) is geared towards the definitions from the records management standards such as ISO 30300 [16], so that it is evident who created or sent the record or document (authenticity) and that it is not possible to deny the creation or submission of a record (non-repudiation). This implies that the main use case of the DIN 31647 (draft) is records management and the preservation of electronic records over a retention period defined by law or business needs. Digital preservation in historical archives is no use case of this standard. DIN 31647 (draft) is based on the ISO standards for records

management and digital preservation for the preservation of evidence of electronic records – a typical use case in e-commerce and e-government. The result is that a trustworthy digital archive, which is also used for the preservation of evidence of electronic records, has to be compliant to DIN 31647 (draft) too, so it will contain functions for the preservation of the digital records itself (usability) and also their evidence. The standard DIN 31647 (draft) is also based on national standards like TR-03125 [8] created by the German Federal Office for Information Security and international technical standards such as RFC 4998 [9], RFC 6283 [10] and ISO 14533 [11-12]. The conclusiveness of electronic records is provided by Evidence Records according to RFC 4998 [9] and RFC 6283 [10] together with supplemental evidence data (signatures and/or (archive) timestamps of the content, verification data such as certificates, CRL-lists or OCSP-responses). These data could be referred to as special fixity information in the PDI of an AIP according to the OAIS [13] which could be described in a special evidence-data description in the provenance information of an AIP.

Based on a vocabulary, oriented on records management standards and DIN 31644, the standard DIN 31647 (draft) describes functional requirements on the preservation of evidence for example:

- Hashing of AIP
  - creation of secure cryptographic hashes
  - ensure securely signed data
  - early hashing of AIP to save their authenticity and integrity
  - sortation, concatenation and canonization of data
- preserve the evidence over long periods of time
- independence from a special technical environment
- full negotiability for unproblematic data exchange between systems and stakeholders by providing self-contained, standardized AIP
  - AIP includes besides the content information descriptive and technical metadata, the supplemental evidence data and the evidence record of the AIP.

In order to archive these requirements it is necessary that the following functions are implicit parts of a system for the preservation of evidence of electronic records:

- collection and verification of supplemental evidence data
- creation of evidence records compliant to RFC 4998 [9] or RFC 6283[10]
- access to evidence records and supplemental evidence data according to the access rules of the digital archive
- verification of evidence records in order to prove the authenticity and integrity of AIP
- preservation by re-signing the archive time stamps or the re-establishment of the involved hash-tree with a new and secure hash algorithm.

To monitor the suitability of the applied cryptographic mechanisms is insofar a main responsibility for a trustworthy digital archive which is used to preserve the evidence of electronic records. A sustainable e-commerce or e-government organization needs to consider the requirements for compliant records management including the verifiability of the authenticity and integrity of records by third parties together with the negotiation, usability and so the reliability of records created in a compliant and trustworthy MSR. In the following the relevant technical standards for the preservation of evidence will be described further.

RFC 4998 and RFC 6283

The preservation of integrity and authenticity of digital records is a very important requirement for long-term archiving systems. Because it is well known that the suitability and security of many cryptographic algorithms decreases with time, it is a challenging task to maintain the integrity and authenticity of archived digital records over very long periods of time.

In a similar manner it is well known that time stamps (cf. [18]) can be used to maintain the integrity and authenticity of digital data or digital signatures over a long time, especially by renewing the time stamps before the previously used signature and hash algorithm becomes insecure. One of the first standards for long term advanced electronic signatures appeared in 2000 ([20], see [4], [5] for recent standards), but they did not provide scalable and cost efficient solutions, because the time stamp renewal would require a new qualified time stamp for each archive data object.

In order to minimize the number of required new qualified time stamps during a time stamp renewal, it is advisable to use Merkle's hash trees as described in [19] and [21] and standardized in [9] as an ASN.1 based Evidence Record Syntax (ERS) and in [10] as an XML based ERS.

The Evidence Record

According to [9] and [10], the Evidence Record Syntax enables processing of several archive objects within a single processing pass using a hash tree technique due to [19] and acquiring only one **Archive Time Stamp** to protect all archive objects. The leaves of the hash tree are hash values of the data objects in a group. An Archive Time Stamp is requested only for the root hash of the hash tree, which ensures efficient processing of large amounts of data.

In order to prove the existence of a single data object, the hash tree can be reduced to a few sets of hash values, called a **Reduced Hashtree**, which are sufficient to prove the existence of a single data object.

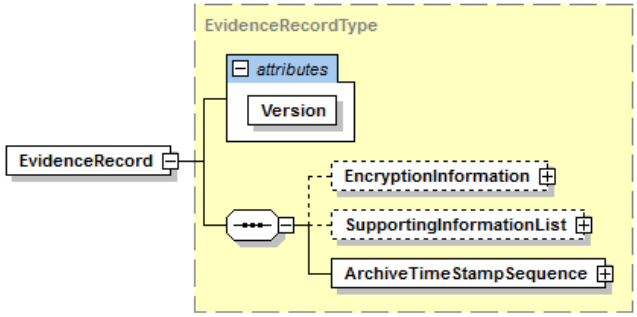

***Figure 3**. An Evidence Record according to RFC 6283 [10]*

The structure of the ASN.1-based Evidence Record according to RFC 4998 is depicted in the following:

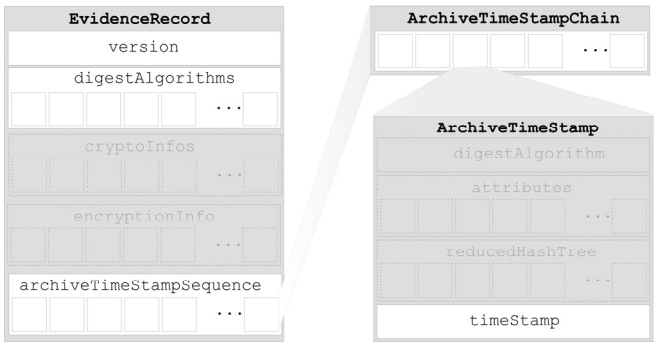

***Figure 4**. An Evidence Record according to RFC 4998 [9]*

If the cryptographic algorithms used to create the Archive Timestamp are at risk to lose its cryptographic suitability, this Archive Timestamp needs to be protected by yet another Archive Timestamp, which is created with suitable new algorithms before the old algorithms lose their cryptographic strength.

For this conservation step one needs to distinguish whether the signature algorithm or the involved hash algorithm is going to become weak.

If only the involved signature algorithm is at risk to lose its suitability, it is sufficient to create a new Archive Timestamp which simply covers the previous one. This process is called **Timestamp Renewal**.

However if the hash algorithm used to build the hash tree is about to lose its suitability, a **Hash-Tree Renewal** is required. In this case the Archive Timestamp and the archived data objects covered by the Archive Timestamp must be hashed with a suitable hash algorithm and time stamped again.

The sequence of Archive Timestamps created during Timestamp Renewal forms an **Archive Timestamp Chain** and the sequence of Archive Timestamp Chains, which is created during corresponding Hash-Tree Renewals, form the **Archive Timestamp Sequence**, which together with some administrative data forms the **Evidence Record**, which is used to prove the authenticity and integrity of the data which is to be protected.

As each new Archive Timestamp in an Archive Timestamp Sequence and Archive Timestamp Chain respectively includes the previous one there is a time-ordered sequence in which the authenticity and integrity of the involved time stamps is preserved as long as each new Archive Timestamp is created while the cryptographic algorithms of the latest existing Archive Timestamp is still suitable.

The standards [9] and [10] define in detail how the generation and verification of Evidence Records and related processes, such as generation and verification of Evidence Records as well as the Timestamp Renewal and Hash-Tree Renewal, need to be performed. Furthermore, the standards define the details of the data formats of the Evidence Records such that they can be exchanged between different archive systems.

CAdES and XAdES

The Cryptographic Message Syntax (CMS) signature format pursuant to [26] is the most commonly used ASN.1 based signature format in practice. Building on this basic CMS structure, specific expansions are defined in [4] and [27] to create an advanced electronic signature based on CMS, which is meant to be conclusive for a long time.

In addition to the CMS based signatures described above, XML based signatures pursuant to [28] are also increasingly being used in practice. The advantage of this signature format is that the specific characteristics of XML based data are taken into account and, thus, for example, one can also sign explicitly defined parts of a document and the signatures themselves can be embedded into the payload data. In [5], specific XML based properties for advanced electronic signatures are defined. The set of properties includes specific attributes for counter signatures, the insertion of timestamps, certificates, and revocation information for example.

Actually, {C/X}AdES defines different forms of {CMS/XML}-based advanced electronic signature profiles, for example the Electronic Signature with Time ({C/X}AdES-T) and the Archival Electronic Signature ({C/X}AdES-A).

A {C/X}AdES Electronic Signature with Time ({C/X}AdES-T) is an electronic signature for which a Trust Service Provider has generated a trusted time token, for example a time stamp, in order to prove that the signature existed at a certain point in time.

It is recommended that a {C/X}AdES-A-Signature is built on the basis of a {C/X}AdES-T-Signature by adding one or more Archive Timestamps, which protect the archive document and related signatures in case the cryptographic algorithms become weak.

In general, a Timestamp Renewal according {C/X}AdES requires a new qualified timestamp for each archive object, but in CAdES it is also possible to use **Evidence Records**, which can be included into a LongTermValidation Attribute.

ISO 14533

The ISO-Standard 14533 consists of two parts:

- Part 1: Long term signature profile for CMS-Advanced Electronic Signatures (CAdES) and
- Part 2: Long term signature profile for XML-Advanced Electronic Signatures (XAdES).

The aim of this standard is to specify the elements, which enable verification of electronic signatures over a long period of time.

Therefore the “signing time shall be identifiable, any illegal alterations of information pertaining to signatures, including the subject of information and validation data, shall be detectable, and interoperability ensured” (cf. [11-12]).

Both parts of ISO 14553 define the following two profiles with respect to {C/X}AdES:

- {C/X}AdES-T profile concerning generation and validation of XAdES-T data;
- {C/X}AdES-A profile concerning generation and validation of XAdES-A data.

In the {C/X}AdES-T profile a “Trusted-Time”- element with a Signature Timestamp or an equivalent method is mandatory.

{C/X}AdES-A is an extension of the {C/X}AdES-T profile, to which specific unsigned attributes are added, for example CertificateValues, RevocationValues, etc. Concerning archiving, at least one type of Archive Timestamp or an Evidence Record must be present in both parts of this international standard.

TR 03125

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) has been developing the Technical Directive TR 03125 (TR-ESOR) [8], which regulates the preservation of evidence of cryptographically signed documents in the context of trustworthy long-term archiving.

The directive is based on the Evidence Record Syntax standards [9-10], the ISO 14533 standards [11-12], the results of the ArchiSig project [21] and on the standardized Open Archival Information System (OAIS) model [13], which provides integrity and authenticity for archived data.

This Technical Guideline TR-ESOR describes a differentiated catalogue of obligatory (shall), recommended (should), and optional (can) requirements with regard to all elements and areas in which there is a need to develop effective, sustainable, and economical technical scenarios for the long term storage of electronically signed documents and data with the preservation of evidence.

The topics addressed in TR-ESOR include

- recommended data and document formats,
- a recommended format for archival information packages,
- recommendations for a reference architecture including specifications of processes, modules and interfaces,
- Conformity test specification for three different certification levels.

The proposed reference architecture (cf. Figure 5) basically consists of the following logical modules:

- ArchiSafe Module,
- Crypto Module,
- ECM-/Storage Module and
- ArchiSig Module.

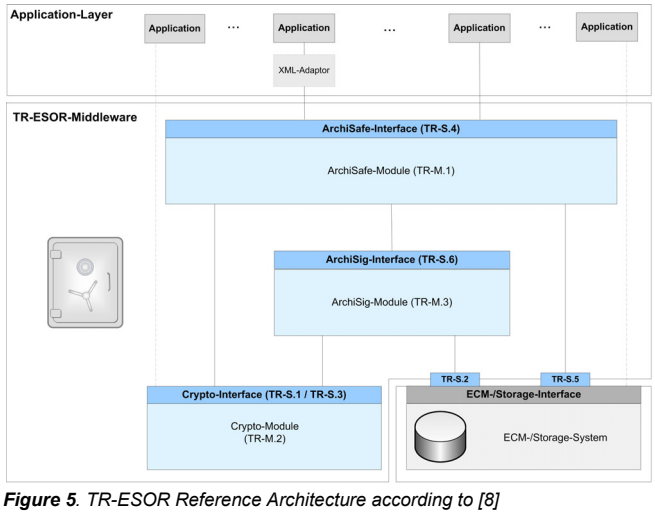

***Figure 5**. TR-ESOR Reference Architecture according to [8]*

The *"ArchiSafe-Module"* (TR-ESOR-M.1) controls the processes and formats on the basis of standardized XML schemas and especially verifies the access rights of the calling entity. The security requirements of this module (especially concerning access control and information flow) are defined in a Common Criteria Protection Profile [22]. It is recommended to certify ArchiSafe products against this Protection Profile in order to guarantee that only reliable requests and archive objects can be sent to the Storage Module.

The *"Crypto-Module"* (TR-ESOR-M.2) supports at least the following cryptographic functions: Generation of hash values, timestamps and (optional) signatures as well as verification of signatures or timestamps along with associated certificate chains and revocation information. The Crypto Interface (cf. Figure 3) is based on internationally standardized interfaces such as [23] and [24] in order to support the interoperability between different Crypto Modules.

The *"ECM-/Storage-Module"* supports at least storage-, retrieval and deletion functions. As the *"ECM-/Storage-Module"* is not part of the TR-ESOR-Middleware, there are no functional requirements specified for this module besides the ability for an exact reproduction of the stored data.

The *"ArchiSig-Module"* (TR-ESOR-M.3) allows to renew the signatures of several documents by issuing just one time stamp using Evidence Records according to [9] and [10]. All documents are hashed and the resulting hash values are merged into a hash tree (cf. [19, 21] and above). Then, a time stamp for the root hash value of the tree is generated. This time stamped hash value allows to prove the validity of all involved documents at the time the time stamp was generated. By iteratively renewing this time stamp before the utilized cryptographic algorithms or parameters become weak or compromised, the validity of the documents is preserved for a potentially arbitrary period of time. This way legal compliance can be achieved. Upon request, the ArchiSig Module uses the stored hash trees and time stamps to generate **Evidence Records** according to [9] or [10]." Furthermore an extended concept which also protects the confidentiality of the stored data is available at [25].

The *„ArchiSafe-Interface"* (TR-ESOR-S. 4) is the standardised interface of the TR-ESOR-Middleware, which is realized as a web service, which builds upon the basic request and response types defined in [24].

Summary and Conclusion

We gave an overview about standards and architectural aspects and procedures for the preservation of evidence and the trustworthiness of digital records by using cryptographic mechanisms, such as electronic signatures and timestamps over very long periods of time.

The integrity and authenticity of the stored data is preserved by efficiently applying time stamps, which are renewed or rehashed in reaction to predictable security threats using the Evidence Record Syntax defined in [9] and [10].

As shown, the Evidence Record Syntax approach is a proof of existence (PoE) at a certain past date, computed over many signed archived data objects or archived data object groups of signed documents together with their signatures, including signed attributes and all other essential components of the signature, providing scalability and cost efficiency.

References

[1] DIN 31644, Information and Documentation – Criteria for Trustworthy Digital Archives, DIN Standard. (2012).

[2] C. Keitel, A. Schoger (Hrsg.): Vertrauenswürdige digitale Langzeitarchivierung nach DIN 31644. Berlin 2013

[3] DIN 31647, Information and Documentation – Preservation of Evidence of Cryptographically Signed Electronic Records (Beweiswerterhaltung kryptographisch signierter Dokumente), DIN Draft Standard. (2013).

[4] ETSI prEN 319 122, CMS Advanced Electronic Signatures (CAdES), Part 1: Core Specification, Draft, available from http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319122-1v003-CAdES-core, (2013)
Part 2: Baseline Profile, Draft, available from http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319122-2v003-CAdES-base, (2013).

[5] ETSI prEN 319 132, XML Advanced Electronic Signatures (XAdES) Part 1: Core Specification, Draft, available from http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319132-1v004-XAdES-core, (2013)
Part 2: Baseline Profile, Draft, available from http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319132-2v004-XAdES-base, (2013).

[6] ETSI prEN 319 521, Policy & Security Requirements for Data Preservation Service Providers, in preparation.

[7] German Federal Law, Act for the Promotion of Electronic Government Administration and for the Amendment of Further Regulations, Federal Law Gazette, BGBL. I No. 43, p. 2749. (2013).

[8] Federal Office for Information Security (BSI): TR 03125 Version 1.1: Preservation of Evidence of Cryptographically Signed Documents (TR-ESOR), available from https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03125/BSITR03125.html, (2011).

[9] IETF RFC 4998, Evidence Record Syntax (ERS), available from http://www.ietf.org/rfc/rfc4998.txt, (2007).

[10] IETF RFC 6283, Extensible Markup Language Evidence Record Syntax (XMLERS), Available from http://www.ietf.org/rfc/rfc6283.txt, (2011).

[11] ISO 14533-1:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES) (2012).

[12] ISO 14533-2:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES) (2012).

[13] ISO 14721:2012, Space data and information transfer systems – Open archival information system (OAIS) – Reference model. (2012).

[14] ISO 15489-1:2001, Information and documentation – Records management – Part 1: General. (2001).

[15] ISO/CD 15489-1 "Information and documentation - Records management - Part 1: General (draft)

[16] ISO 30300:2011 "Information and documentation - Management systems for records -Fundamentals and vocabulary" (2011)

[17] ISO 30301:2011, Information and documentation – Management systems for records – Requirements. (2011).

[18] S. Haber and W. S. Stornetta, How to time-stamp a digital document, Journal of Cryptology, vol. 3, no. 2, p. 99–111, 1991.

[19] R. C. Merkle, Protocols for public key cryptosystems, in Symposium on Security and Privacy, Oakland, CA, USA, p. 122–134.(1980).

[20] European Telecommunications Standards Institute (ETSI), Electronic Signatures and Infrastructures (ESI) – Electronic Signature Formats, ETSI Standard ES 201 733, Version 1.1.3, (2000)

[21] W. Zimmer, T. Langkabel, and C. Hentrich, Archisafe: Legally compliant electronic storage, IT Professional, vol. 10, no. 4, pp. 26–33. (2008).

[22] Physikalisch-Technische Bundesanstalt (PTB): Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Legally compliant Long-Term Preservation of Electronic Documents (ACM_PP).

[23] Federal Office for Information Security (BSI), eCard-API-Framework – Part 1 – Overview and general definitions, BSI TR-03112-1, Version 1.1.2 . (2012)

[24] OASIS, Digital signature service core protocols, elements, and bindings, version 1.0, http://docs.oasis-open.org/dss/v1.0/oasis-dss-corespec-v1.0-os.pdf, (2007).

[25] D. Hühnlein, U. Korte, L. Langer, A. Wiesmaier, A Comprehensive Reference Architecture for Trustworthy Long-Term Archiving of Sensitive Data, in Khaldoun Al Agha and Mohamad Badra and Gregory B. Newby, Editor, NTMS 2009, 3rd International Conference on New Technologies, Mobility and Security, 20-23 December 2009, Cairo, Egypt , Seite 1-5, IEEE. (2009).

[26] R. Housley, IETF RFC 5652, "Cryptographic Message Syntax (CMS), http://www.ietf.org/rfc/rfc5652.txt , (2009).

[27] D. Pinkas, J. Ross, N. Pope, IETF RFC 5126, CMS Advanced Electronic Signatures (CAdES), http://www.ietf.org/rfc/rfc5126.txt (2008).

[28] D. Eastlake, et al., XML Signature Syntax and Processing (Second Edition), W3C Recommendation, http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/ (2008).

[29] P. Maniatis and M. Baker, Enabling the archival storage of signed documents, in Proceedings of the 2002 Conference on File and Storage Technologies (FAST). USENIX, 2002, p. 1–14. (2002).

Author Biography

Steffen Schwalm works as Business Advisor for BearingPoint Management & Technology Consultants. He is an expert in preservation of evidence and trust for electronic records and records management. He has 10 years of professional experiences and participates in standardization groups at ISO & DIN e.g. ISO 15489 or DIN 31647. Steffen Schwalm studied information sciences and (co-)authored 4 books, more than 25 articles for journals or proceedings and frequently gives lectures at relevant conferences.

Ulrike Korte has been working for the Federal Office for Information Security (BSI) in Bonn since 2004. She obtained her Ph.D. of mathematics in 1981 from the University of Münster and has been working with data security since then. Ulrike Korte (co-)authored one book and more than 50 articles for journals and conferences and participated in professional standardisation bodies, as for example "ISO/TC 154 UN/ECE/Joint Syntax Working Group" and "ISO/TC 154 Long term signature profiles".

Detlef Hühnlein is CEO of ecsec GmbH and has more than fifteen years of professional experience in the area of IT-security, received a doctoral degree in cryptography from TU Darmstadt, gives lectures about electronic signatures, internet security and identity management at universities, (co-)authored more than 70 papers for refereed journals and conferences, gives talks at national and international IT security events and has been actively involved in different standardization initiatives at DIN, CEN, ISO and OASIS.