Long-term Preservation of Validity of Electronically Signed Records

Hrvoje Brzica[*]
Boris Herceg[*]
Financial Agency – FINA
Ulica grada Vukovara 70, 10000 Zagreb, Croatia
Hrvoje.Brzica@fina.hr, Boris.Herceg@fina.hr

Hrvoje Stančić
Department of Information and Communication Sciences,
Faculty of Humanities and Social Sciences, University of Zagreb
Ivana Lučića 3, Zagreb, Croatia
hstancic@ffzg.hr

Summary

The authors explain the context in which electronic records are being preserved. They explain the concept of authentic electronic records and proceed with the analysis of the technologies supporting trust in electronic records. They start by explaining the Public Key Infrastructure as the requirement for electronic signatures, digital certificates, the concept of non-repudiation, trusted archive service, timestamps and trusted digital timestamping. Further, they analyse formats of electronic signatures – XMLDSig, XAdES, CAdES, PAdES – and their possible influence on the long-term preservation of validity of electronically signed records. The authors conclude that although strict requirements of certain types of electronic signatures can ensure authenticity, integrity and non-repudiation of preserved records, they will still require preservation action on the level of medium and files.

Key words: electronic signature, digital certificate, non-repudiation, trusted archive service, timestamp, XMLDSig, XAdES, CAdES, PAdES

Introduction

Digital documents are being created in every segment of modern business. Those documents may or may not be part of a document management system. Increasingly they are not printed and signed but are digitally signed instead. At that moment they become records. They are used in the process of business and later, when they lose their immediate business value, are archived and may or

[*] The positions put forward in this article are solely those of the authors' and do not necessarily reflect the positions of FINA.

may not become part of a records management system and stored within a digital archive solution. If those records are to be preserved in the long-term their characteristics of authenticity, reliability, integrity and usability[1] have to be preserved.

"Authenticity is not a single concept, but involves different aspects that can be associated with an object:

- A traceable path from the object's original to its current ownership.
- Measures and techniques for safeguarding against and/or recognizing modifications.
- Techniques for establishing the use of original materials.

Usage and context define how these aspects are defined for individual classes of objects."[2] Therefore, as Duranti says, "a document is authentic if it can be demonstrated that it is precisely as it was when first transmitted or set aside for preservation, and if its reliability, i.e., the trustworthiness it had at that moment, has been maintained intact."[3]

This shows that the concept of long-term preservation of digital records with the abovementioned characteristics requires a complex digital solution. The aim of this paper is to give a context in which modern digital documents and records are being created, to explain the technologies required to support that process and to analyse their influence on long-term preservation of validity of electronically signed records. Therefore, the concepts of electronic signatures, digital certificates, non-repudiation, trusted archive service, timestamps and trusted digital timestamping will be explained. For better understanding of those concepts, the concept of Public Key Infrastructure needs to be shortly explained.

"Public Key Infrastructure (PKI) represents complex information infrastructure, which is used to manage electronic identities. Basis of PKI relies on asymmetric encryption. Asymmetric encryption actually relies on mathematically related key pair, one called the public key, and another called private key, generated to be used together. (...) The private key is kept secret and used only by its owner, while public key is made available to anyone who wants it."[4] Modern systems can easily use the keys with length of 2048 characters which are impossible to break even by todays supercomputers.

[1] As defined by ISO 15489: Information and documentation – Records management, 2001.

[2] Van Diessen, Raymond J. and van der Werf-Davelaar, Titia, *Authenticity in a Digital Environment*, IBM / Koninklijke Bibliotheek Long-Term Preservation Study Report Series, No. 2, IBM Netherlands, Amsterdam, December 2002, p. 3, http://www.kb.nl/sites/default/files/docs/2-authenticity.pdf (22.2.2013)

[3] Duranti, Luciana, The Concept of Electronic Record, in: Duranti, Luciana, Eastwood, Terry and MacNeil Heather, *Preservation of Integrity of Electronic Records*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002, p. 27.

[4] Jacobs, J., Clemmer, L., Dalton, M., Rogers, R., Posluns, J., *SSCP Study Guide*, Syngress Publishing, 2003, pp. 330-331.

Technologies and concepts supporting trust in electronic records

Electronic signature

There are two types of electronic signatures – basic (usually referred to just as "electronic signature") and advanced. The European Telecommunications Standards Institute (ETSI) 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."[5] European legislation in the Directive 1999/93/EC states that an electronic signature needs to meet the following requirements in order to become an advanced electronic signature[6]:

a) it is uniquely linked to the signatory[7];
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 is detectable.

Digital certificates

Digital certificates are digital records used for confirming the identity of a person, an organisation or a machine. Digital certificate is valid during certain period of time and contains several additional elements. The Directive 1999/93/EC allows issuing of the so called *qualified certificate* which is based on the RFC 3039 standard and implements the concept of non-repudiation. The qualified certificate must in particular include[8]:

a) an indication that the certificate is issued as a qualified certificate;
b) the identification of the certification-service-provider and the State in which it is established;
c) the name of the signatory or a pseudonym, which shall be identified as such;

[5] Electronic signature, ETSI, 2012, http://www.etsi.org/index.php/technologies-clusters/ technologies/security/electronic-signature (9.7.2013)

[6] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 013, 19 January 2000, pp. 12-20, http://europa.eu/legislation_summaries/information_society/other_policies/l24118_en.htm (11. 7.2013)

[7] "A person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents." (Directive 1999/93/EC)

[8] Directive 1999/93/EC.

d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
e) signature-verification data which correspond to signature-creation data under the control of the signatory;
f) an indication of the beginning and end of the period of validity of the certificate;
g) the identity code of the certificate;
h) the advanced electronic signature of the certification-service-provider issuing it;
i) limitations on the scope of use of the certificate, if applicable; and
j) limits on the value of transactions for which the certificate can be used, if applicable.

Certification authority and registration authority
In the PKI infrastructure digital certificates are issued and revoked by the Certification Authority (CA). CA is organised as a hierarchy within which a Root CA is used as the highest entity, trusting itself, while all other, hierarchically lower entities trust the Root CA. The idea is that every identified entity receives digital signature, i.e. a certificate of its public key which, in turn, can be used for confirm its identity. The procedure is that CA uses its private key to sign the digital certificate of an entity, and the identity of that entity can be checked by using CA's public key. It is important to mention that, upon the request for certification by an entity, "a CA checks with a Registration Authority (RA)[9] to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate."[10]

Non-repudiation

Non-repudiation is a characteristic of a record that prevents any signatory to deny the action taken or the content of a record. In the Croatian legislation non-repudiation is associated with the advanced digital signature which is based upon qualified certificate. For a record to achieve and preserve characteristic of non-repudiation it is necessary to ensure:

1. digital identity of signatories,
2. real-time revocation of digital signature rights,

[9] Registration authority, as a part of PKI infrastructure, is "an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it." Search Security, s.n. registration authority, January 2006, http://searchsecurity.techtarget.com/definition/registration-authority (9.7.2013)

[10] Search Security, s.n. certificate authority (CA), June 2007, http://searchsecurity.techtarget.com/definition/certificate-authority (9.7.2013)

3. time-stamping of digital signatures after checking the list of revoked certificates, which ensures the validity of electronic signature at the time of signing, and
4. secure long-term preservation.

Trusted archive service

Dumortier and Eynde explain that a trusted archive service (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. To achieve this goal in the best possible way, the TAS must only accept documents in a format that can still be understood when the format will no longer be in use. Only open file formats that are vendor-independent qualify for long term archiving. (...) Every TAS must therefore publish a list of supported document formats. Such a list may be exhaustive or very restricted. Every time a document is submitted, the TAS must check the format before accepting it for archiving."[11]

Timestamp and trusted digital timestamping

According to Wallace et al. 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.[12] Ćosić and Bača 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."[13]

Formats of electronic signatures

In the analysis so far the technologies and concepts supporting trust in electronic records were explained. It was shown that the concept of electronic signature can be viewed as the basis for developing all other technologies. Further,

[11] Dumortier, Jos and Eynde, Sofie Van den, Electronic Signatures and Trusted Archival Services, DAVID Project (2000-2003), p. 7, http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf (8.7.2013)

[12] Wallace, C., Pordesch, U. and Brandner R., Long-Term Archive Service Requirements, IETF Trust, 2007, p. 5, http://tools.ietf.org/pdf/rfc4810.pdf (9.7.2013)

[13] Ćosić, Jasmin and Bača, Miroslav, (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp, MIPRO – Proceedings of the 33rd International Convention, 2010, pp. 1227-1228, http://czb.foi.hr/upload/datoteke/10_400%281%29.pdf (9.7.2013)

the realisation of digital signatures will be explained through analysis of the most important formats of electronic signatures – XMLDSig, XAdES, CAdES and PAdES.

XMLDSig

XML (Extensible Markup Language) Signature is defined by the W3C Recommendation[14]. In the literature it is referred to as XMLDSig, XML-DSig or XML-Sig. The W3C Recommendation states that "XML Signatures can be applied to any digital content (data object), including XML. An XML Signature may be applied to the content of one or more resources." One can differentiate between[15]:

- detached signature – an XML signature used to sign a resource outside its containing XML document, i.e. the signature is over content external to the `Signature` element;
- enveloped signature – signature is child; it is used to sign some part of its containing document, i.e. the signature is over content found within an `Object` element of the signature itself:
- enveloping signature – signature is parent; it contains the signed data within itself, i.e. the signature is over the XML content that contains the signature as an element. The content provides the root XML document element. Obviously, enveloped signatures must take care not to include their own value in the calculation of the `SignatureValue`.

"XML Signatures are applied to arbitrary digital content (data objects) via an indirection. Data objects are digested, the resulting value is placed in an element (with other information) and that element is then digested and cryptographically signed."[16]

XAdES

XAdES (XML Advanced Electronic Signature) "extends XMLDSig specification into the domain of non-repudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European 'Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures' and incorporate additional useful information in common uses cases. This includes evidence as to its validity even if the signer or verifying party

[14] XML Signature Syntax and Processing (Second Edition), W3C Recommendation, The Internet Society & W3C, 10 June 2008, http://www.w3.org/TR/xmldsig-core/ (10.7.2013)

[15] XML Signature, Wikipedia, June 2013, http://en.wikipedia.org/wiki/XML_Signature (10.7. 2013).
XML Signature Syntax and Processing (Second Edition), W3C Recommendation.

[16] XML Signature Syntax and Processing (Second Edition), W3C Recommendation.

later attempts to deny (repudiates) the validity of the signature. An advanced electronic signature aligned with the present document (i.e. XAdES specification) can, in consequence, be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later."[17] In relation to XMLDSig, XAdES specification adds six additional, mutually nested, forms (see Figure 1):

1. XAdES (also referred to as XAdES-BES – basic electronic signature) – basic form defining elements for authentication and protection of integrity of records but not providing non-repudiation of its existence.
2. XAdES-T (Timestamp) – addition of the timestamp ensures non-repudiation.
3. XAdES-C (Complete validation data) – builds up on the XAdES-T by adding references to the set of data supporting the validation of the electronic signature (i.e. the references to the certification path and its associated revocation status information). This form is useful for those situations where such information is archived by an external source, like a trusted service provider.
4. XAdES-X (eXtended validation data) – builds up on XAdES-C by adding timestamps to protect against the risk that any keys used in the certificate chain or in the revocation status information may be compromised.
5. XAdES-X-L (eXtended validation data incorporated for the Long term) – builds up on XAdES-X by adding the validation data (i.e. certificates and revocation values) for those situations where the validation data are not stored elsewhere for the long-term.
6. XAdES-A (Archiving validation data) – builds up on XAdES-X-L by adding time-stamps for archiving signatures

CAdES

CAdES (CMS Advanced Electronic Signatures) is a set of extensions to CMS (Cryptographic Message Syntax) signed data. It "defines a number of electronic signature formats, including electronic signatures that can remain valid over long periods. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the electronic signature."[18] Similar to XAdES, CAdES specification defines six profiles, each building up on the previous one: CAdES – basic form, CAdES-T (Timestamp), CAdES-C (Complete), CAdES-X (eXtended), CAdES-X-L (eXtended Long-term) and CAdES-A (Archival). The difference between the two specifications

[17] XML Advanced Electronic Signatures (XAdES), W3C Note 20 February 2003, ETSI, 2003, http://www.w3.org/TR/XAdES/ (10.7.2013)

[18] CMS Advanced Electronic Signatures (CAdES) Technical Specification, ETSI TS 101 733 v1.7.4, July 2008, p. 8, http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/01.07.04_60/ts_101733v010704p.pdf (10.7.2013)

is that while CAdES renders signature as binary data, XAdES provides an XML solution.

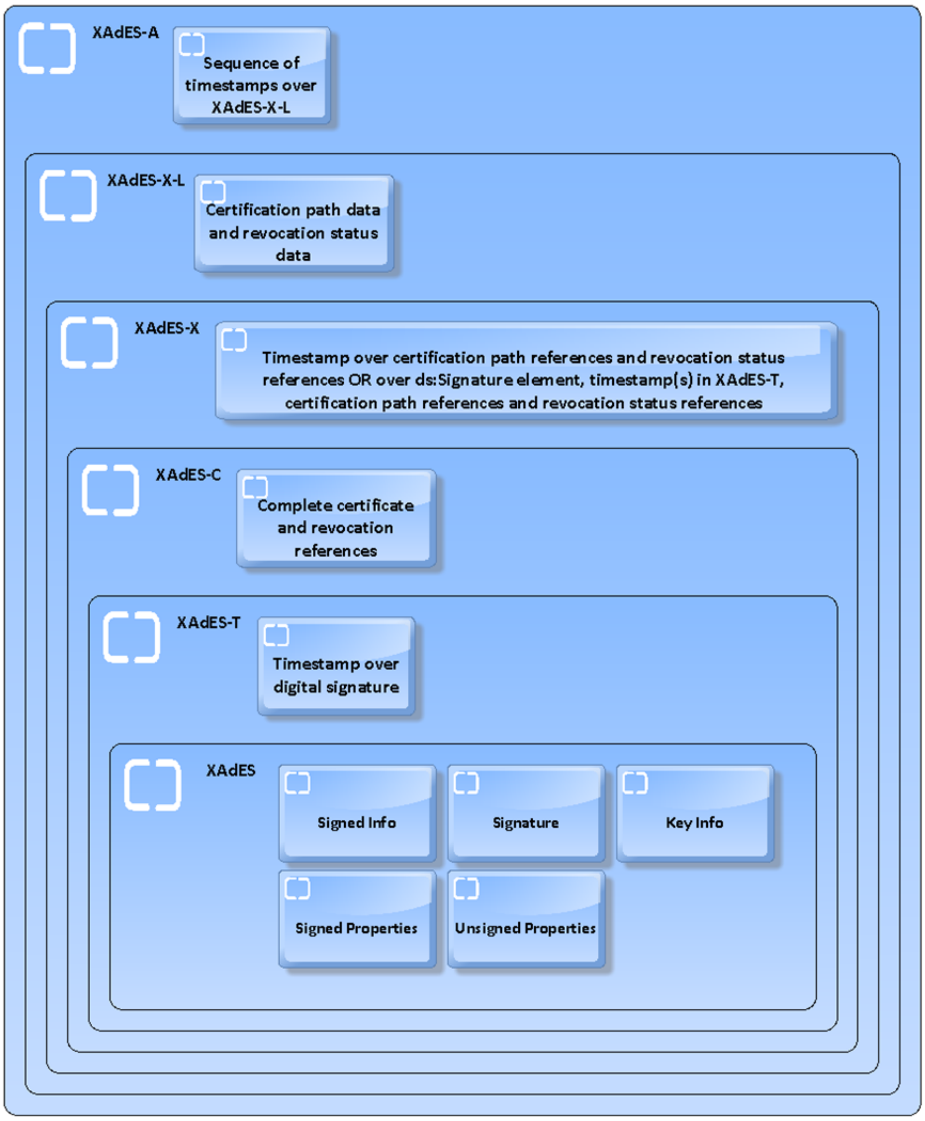

XAdES-A
Sequence of timestamps over XAdES-X-L
XAdES-X-L
Certification path data and revocation status data
XAdES-X
Timestamp over certification path references and revocation status references OR over ds:Signature element, timestamp(s) in XAdES-T, certification path references and revocation status references
XAdES-C
Complete certificate and revocation references
XAdES-T
Timestamp over digital signature
XAdES
Signed Info
Signature
Key Info
Signed Properties
Unsigned Properties

Figure 1: Structure of XAdES specification forms

PAdES

PAdES (PDF Advanced Electronic Signature) "articulates the same capabilities featured in CAdES and XAdES for PDF. (...) PAdES differs from CAdES and XAdES in that it applies only to PDF documents and defines requirements that PDF viewing and editing software must follow when using digital signatures in

PDF documents. As the standard for viewable documents, PDF also defines how a signature can be displayed as it might with an ink-on-paper signature at a particular position on a particular page, and how digital signatures can be integrated with the form-filling features of PDF. This is a key factor that distinguishes it from CAdES and XAdES, which are more suited for applications that may not involve human-readable documents."[19] PAdES specification is realised in 6 parts:

Part 1 – PAdES Overview – a framework document for PAdES[20]

Part 2 – PAdES Basic – Profile based on ISO 32000-1: specifies a PDF signature as specified in ISO 32000-1:2008 that enables greater interoperability for PDF signatures by providing additional restrictions beyond those of ISO 32000-1.[21]

Part 3 – PAdES Enhanced: incorporates the signature time-stamp attribute as optional making the signature effectively a CAdES-T form.[22]

Part 4 – PAdES Long Term: uses an extension to ISO 32000-1 called Document Security Store (DSS) to carry such validation data as necessary to validate a signature, optionally with Validation Related Information (VRI) which relates the validation data to a specific signature.[23]

Part 5 – PAdES for XML Content: profile for usage of arbitrary signed (with XAdES signatures) XML document that is embedded within a PDF file, for providing integrity, authentication and non-repudiation services on the data objects that are signed with the XAdES signature.[24]

Part 6 – Visual Representations of Electronic Signatures: specifies requirements and recommendations for the visual representations of advanced electronic signatures (AdES) in PDFs[25]. The signature appearance is created by the signer and any identification included in the signature appearance is not directly verifiable by the AdES signature. However, this information may be visually checked against the visual representation of the electronic signature (AdES) verification.[26]

[19] The AdES family of standards: CAdES, XAdES, and PAdES. Implementation guidance for using electronic signatures in the European Union, White paper, Adobe Systems, 2009, p. 5, http://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf (10.7.2013)

[20] PAdES. Part 1.

[21] PAdES. Part 2, p. 8.

[22] PAdES. Part 3, p. 7.

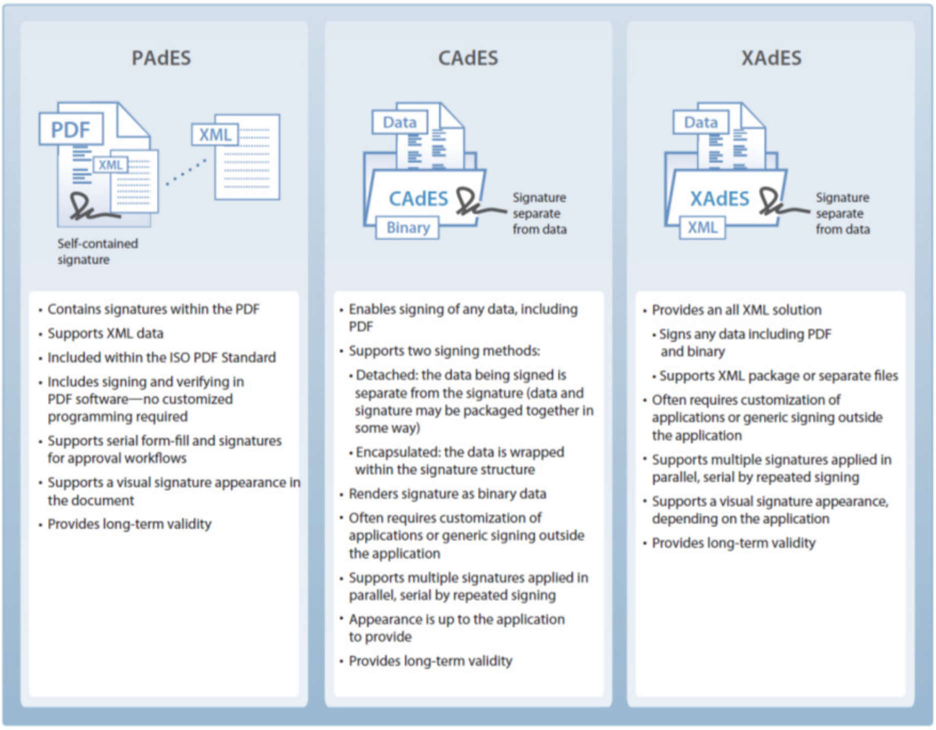
[23] PAdES. Part 4, p. 8.

[24] PAdES. Part 5, p. 9.

[25] PAdES. Part 6, p. 5.

[26] Ibid., p. 7.

ETSI is developing Part 7 of the PAdES specification: Baseline Profile which will address e-Invoicing. The profile will identify a common set of options that are appropriate for maximizing interoperability between PAdES signatures. At the moment of writing this paper, Part 7 was still in the form of early draft.



PAdES

- Contains signatures within the PDF
- Supports XML data
- Included within the ISO PDF Standard
- Includes signing and verifying in PDF software—no customized programming required
- Supports serial form-fill and signatures for approval workflows
- Supports a visual signature appearance in the document
- Provides long-term validity

CAdES

- Enables signing of any data, including PDF
- Supports two signing methods:
  - Detached: the data being signed is separate from the signature (data and signature may be packaged together in some way)
  - Encapsulated: the data is wrapped within the signature structure
- Renders signature as binary data
- Often requires customization of applications or generic signing outside the application
- Supports multiple signatures applied in parallel, serial by repeated signing
- Appearance is up to the application to provide
- Provides long-term validity

XAdES

- Provides an all XML solution
  - Signs any data including PDF and binary
  - Supports XML package or separate files
- Often requires customization of applications or generic signing outside the application
- Supports multiple signatures applied in parallel, serial by repeated signing
- Supports a visual signature appearance, depending on the application
- Provides long-term validity

Figure 2: Comparison of PAdES, CAdES, and XAdES[27]

Conclusion

The analysis of technologies and concepts supporting trust in electronic records as well as the formats of digital signatures showed important issues that should be addressed when long-term preservation of authentic electronic records is considered. Setting up a digital archive in accordance with the discussed Directive 1999/93/EC and European Telecommunications Standards Institute's advance digital signature specifications can ensure authenticity, integrity and non-repudiation of preserved records signed by advance digital signatures because they enable possibility of checking the validation chain during the long-term preservation. However, it is important to keep in mind that majority of solutions explained in this article try to tackle only the problem of long-term preservation of electronic signatures, not the actual documents that are signed.

[27] The AdES family of standards, p. 7.

Therefore, long-term preservation of electronically signed records will, in time, still require some kind of preservation action, e.g. emulation or migration. Ideally, establishing a trusted archive service based both on advance digital signature specifications and proactive approach to digital preservation should prove the best solution.

References

Boudrez, Filip, Digital Signatures and Electronic Records, Archival Science 7(2), 2007, pp. 179-193., http://www.edavid.be/docs/digitalsignatures.pdf (12.7.2013)

CMS Advanced Electronic Signatures (CAdES) Technical Specification, ETSI TS 101 733 v1.7.4, July 2008, http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/01.07.04_60/ts_101733v010704p.pdf (10.7.2013)

Ćosić, Jasmin and Bača, Miroslav, (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp, MIPRO - Proceedings of the 33rd International Convention, 2010, pp. 1226-1230, http://czb.foi.hr/upload/datoteke/10_400%281%29.pdf (9.7.2013)

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 013, 19 January 2000, pp. 12-20, http://europa.eu/legislation_summaries/information_society/other_policies/l24118_en.htm (11.7.2013)

Dumortier, Jos and Eynde, Sofie Van den, Electronic Signatures and Trusted Archival Services, DAVID Project (2000-2003), pp. 1-9, http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf (8.7.2013)

Duranti, Luciana, The Concept of Electronic Record, in: Duranti, Luciana, Eastwood, Terry and MacNeil Heather, Preservation of Integrity of Electronic Records, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002

Electronic signature, ETSI, 2012, http://www.etsi.org/index.php/technologies-clusters/technologies/security/electronic-signature (9.7.2013)

ISO 15489: Information and documentation – Records management, 2001.

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

PAdES – PDF Advanced Electronic Signature Profiles. Part 1: PAdES Overview - a framework document for PAdES, Technical Specification, ETSI TS 102 778-1 V1.1.1, July 2009, http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf (10.7.2013)

PAdES. Part 2: PAdES Basic - Profile based on ISO 32000-1, Technical Specification, ETSI TS 102 778-2 V1.2.1, July 2009, http://www.etsi.org/deliver/etsi_ts/102700_102799/10277802/01.02.01_60/ts_10277802v010201p.pdf (10.7.2013)

PAdES. Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles, Technical Specification, ETSI TS 102 778-3 V1.2.1, July 2010, http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/ts_10277803v010201p.pdf (10.7.2013)

PAdES. Part 4: PAdES Long Term - PAdES-LTV Profile, Technical Specification, ETSI TS 102 778-4 V1.1.2, December 2009, http://www.etsi.org/deliver/etsi_ts/102700_102799/10277804/01.01.02_60/ts_10277804v010102p.pdf (10.7.2013)

PAdES. Part 5: PAdES for XML Content - Profiles for XAdES signatures, Technical Specification, ETSI TS 102 778-5 V1.1.2, December 2009, http://www.etsi.org/deliver/etsi_ts/102700_102799/10277805/01.01.02_60/ts_10277805v010102p.pdf (10.7.2013)

PAdES. Part 6: Visual Representations of Electronic Signatures, Technical Specification, ETSI TS 102 778-6 V1.1.1, July 2010, http://www.etsi.org/deliver/etsi_ts/102700_102799/10277806/01.01.01_60/ts_10277806v010101p.pdf (10.7.2013)

Search Security, s.n. certificate authority (CA), June 2007, http://searchsecurity.techtarget.com/definition/certificate-authority (9.7.2013)

Search Security, s.n. registration authority, January 2006, http://searchsecurity.techtarget.com/definition/registration-authority (9.7.2013)

The AdES family of standards: CAdES, XAdES, and PAdES. Implementation guidance for using electronic signatures in the European Union, White paper, Adobe Systems, 2009, http://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf (10.7.2013)

Van Diessen, Raymond J. and van der Werf-Davelaar, Titia, *Authenticity in a Digital Environment*, IBM / Koninklijke Bibliotheek Long-Term Preservation Study Report Series, No. 2, IBM Netherlands, Amsterdam, December 2002, http://www.kb.nl/sites/default/files/docs/2-authenticity.pdf (22.2.2013)

Wallace, C., Pordesch, U. and Brandner R., Long-Term Archive Service Requirements, IETF Trust, 2007, pp. 1-17, http://tools.ietf.org/pdf/rfc4810.pdf (9.7.2013)

Wikipedia, XML Signature, June 2013, http://en.wikipedia.org/wiki/XML_Signature (10.7.2013)

XML Advanced Electronic Signatures (XAdES), Technical Specification, ETSI TS 101 903 v1.2.2, April 2004, http://uri.etsi.org/01903/v1.2.2/ts_101903v010202p.pdf (10.7.2013)

XML Advanced Electronic Signatures (XAdES), W3C Note 20 February 2003, ETSI, 2003, http://www.w3.org/TR/XAdES/ (10.7.2013)

XML Signature Syntax and Processing (Second Edition), W3C Recommendation, The Internet Society & W3C, 10 June 2008, http://www.w3.org/TR/xmldsig-core/ (10.7.2013)