ETSI SR 019 510 V1.1.1 (2017-05)

Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures

Reference

DSR/ESI-0019510

Keywords

electronic preservation, electronic signature, security, trusted services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

The standard (or standards) extracts (ISO 14721:2012: "Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model", ISO 14533-1:2014: "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)", 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)") are replicated with AFNOR's consent. Only the complete and original text as released by AFNOR Editions - accessible on the website www.boutique.afnor.org - has normative value.

Foreword

This Special Report (SR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

On the one hand, digital signatures as well as time-stamps based on cryptographic mechanisms are increasingly used in our everyday life.

On the other hand it is well known, that the strength and suitability of cryptographic mechanisms is a function of time and one needs to apply suitable preservation mechanisms, which are able to maintain the validity status of a signed object over long periods of time, which may involve the application of different storage technologies and cryptographic algorithms.

The need for long-term preservation is acknowledged amongst others in the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market [i.1], as can be seen in recital (61):

"*This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.*"

Furthermore Article 34 of the Regulation (EU) No 910/2014 [i.1] states that "*a qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period*" and that "*the Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures.*"

The present document provides an overview of preservation mechanisms which can be used to preserve the validity status of digital signatures or to preserve objects using digital signature techniques. It may be used to support all kinds of preservation services including for example qualified preservation service for qualified electronic signatures according to Article 34 of the Regulation (EU) No 910/2014 [i.1], and mutatis mutandis for qualified preservation service for qualified electronic seals according to Article 40 of this regulation.

1 Scope

The present document provides a scoping study for long-term data preservation (including preservation of/with digital signatures).

The present document aims at supporting preservation services in different regulatory frameworks.

NOTE 1: Specifically, but not exclusively, the preservation service addressed in the present document aims at supporting qualified preservation service for qualified electronic signatures or seals as per Regulation (EU) No 910/2014 [i.1].

NOTE 2: Specifically, but not exclusively, digital signatures in the present document cover electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1].

The present document covers two main cases:

1) The preservation of the **validity status** of the **digital signatures** (using time-stamps, Evidence Records, etc.) and of the associated signed data

NOTE 3: A qualified preservation service for qualified electronic signatures or seals as per Regulation (EU) No 910/2014 [i.1] for which the status of the technical validity needs to be preserved, is covered in this case. This special report cannot say anything about the legal validity of a signature.

NOTE 4: The validity of a signature means the status of the signature that will not change over time, e.g. if a signature was valid (TOTAL_PASSED according to ETSI EN 319 102-1 [i.9]) or invalid (TOTAL_FAILED and in certain cases for INDETERMINATE according to ETSI EN 319 102-1 [i.9]). The long-term preservation of the validity status includes the preservation of the bits of:

- the documents being signed; and/or
- other digital objects like certificates, OCSPs, Time-Stamp Tokens, etc.

2) Preservation of the integrity of bits of digital objects, whether they are signed or not, **using digital signature techniques** (digital signatures, time-stamp tokens, Evidence Records, etc.)

NOTE 5: In this case, if the main object to be preserved is a signature, it is treated in the same way as any other file.

NOTE 6: The preservation of the integrity of bits of digital object not using digital signature techniques is not in the scope of the present document.

In addition, the present document provides an inventory of existing standards and selected legal frameworks on the topic of preservation services.

The present document provides as well a proposal for a framework of standards.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73-114.

[i.2] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.3] ETSI TR 101 533-2: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors".

[i.4] ETSI TS 101 733 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.5] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.6] ETSI TS 102 573: "Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects".

[i.7] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.8] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.9] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.10] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.11] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.12] ETSI TS 119 122-3: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES".

[i.13] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.14] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.15] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.16] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.17] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers".

[i.18] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

[i.19] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[i.20] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists".

[i.21] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.22] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.23] ISO 13527 (2010): "Space data and information transfer systems -- XML formatted data unit (XFDU) structure and construction rules".

[i.24] ISO 14533-1 (2014): "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)".

[i.25] 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)".

[i.26] ISO 14721 (2012): "Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model".

[i.27] ISO 15489-1 (2001): "Information and documentation -- Records management -- Part 1: General".

[i.28] ISO 19005-3 (2012): "Document management - Electronic document file format for long-term preservation - Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)".

[i.29] ISO/IEC 21320-1 (2015): "Information technology -- Document Container File -- Part 1: Core".

[i.30] ISO/IEC 27000 (2016): "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.31] ISO/IEC 27040 (2015): "Information technology -- Security techniques -- Storage security".

[i.32] IETF RFC 3126: "Electronic Signature Formats for long term electronic signatures".

[i.33] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[i.34] IETF RFC 4810: "Long-Term Archive Service Requirements".

[i.35] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.36] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.37] IETF RFC 5698: "Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC)".

[i.38] IETF RFC 5816: "ESSCertIDv2 Update for RFC 3161".

[i.39] IETF RFC 6283 (2011): "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.40] IETF RFC 6838: "Media Type Specifications and Registration Procedures".

[i.41] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.42] AFNOR NF Z40-020: "Spécifications fonctionnelles d'un composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps", 2012.

[i.43] BSI TR-03125 (2015): "Preservation of Evidence of Cryptographically Signed Documents (TR-ESOR)".

NOTE: Available at https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03125/BSITR03125.html.

[i.44] BSI TR-03125- C.1 (2015): "Conformity Test Specification (Level 1 - Functional conformity) (TR-ESOR-C.1)".

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_C1_V1_2.pdf?__blob=publicationFile&v=1.

[i.45] BSI TR-03125-C.2 (2015): "Conformity Test Specification (Level 2 - Technical Conformity) (TR-ESOR-C.2)".

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_C2_V1_2.pdf?__blob=publicationFile&v=1.

[i.46] BSI TR-03125-C.3 (2015): "Technical Conformity Test Specification (Level 3 - Conformity with the German Federal Agency Profiling) (TR-ESOR-C.3)".

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_C3_V1_2.pdf?__blob=publicationFile&v=1.

[i.47] BSI TR- 03125-E (2015): "Concretisation of the Interfaces on the Basis of the eCard-API-Framework (TR-ESOR-E)".

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR-E_V1_2_EN.pdf?__blob=publicationFile&v=4.

[i.48] BSI TR-03125-F (2015): "Preservation of Evidence of Cryptographically signed Documents, Formats (TR-ESOR-F)".

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR-F_V1_2_EN.pdf?__blob=publicationFile&v=2.

[i.49] BSI TR- 03125-S (2015): "Interface Specifications (TR-ESOR-S)".

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR-S_V1_2_EN.pdf?__blob=publicationFile&v=2.

[i.50] BSI-CC-PP-0049 (2014): "Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents".

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0049+PP0049_2014.html.

[i.51] BSI-CC-PP-0049 (2008), National Metrology Institute of Germany (Physikalisch-Technische Bundesanstalt): "Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents (ACM-PP)".

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0049b_pdf.pdf.

[i.52] V. L. Lemieux: "Trusting Records: Is Blockchain Technology the Answer?", Records Management Journal 26.2.2016.

[i.53] R. Merkle: "Protocols for Public Key Cryptosystems", Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA), 1980, pages 122-134.

[i.54] A. Miller, A. Juels, E. Shi, B. Parno, & J. Katz: Permacoin: "Repurposing bitcoin work for data preservation", In 2014 IEEE Symposium on Security and Privacy, 2014, pages 475-490).

[i.55] Martín Vigil, Johannes Buchmann, Daniel Cabarcas, Christian Weinert, and Alexander Wiesmaier: "Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving", Comput. Secur. 50, 2015.

[i.56] Moreq10: "Model Requirements for the Management of Electronic Records - Moreq10, Modular Requirements for Records Systems", Version 1.1 (English), ISBN: 978-92-79-18519-9.

NOTE: Available at http://www.moreq.info/index.php.

[i.57] OASIS (2007): "Digital signature service core protocols, elements, and bindings", version 1.0.

NOTE: Available at http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf, 2007.

[i.58] W3C: "Extensible Markup Language (XML) 1.0 (Fifth Edition)", W3C Recommendation 26 November 2008.

NOTE: Available at https://www.w3.org/TR/REC-xml/.

[i.59] ETSI TS 119 431: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

[i.60] ISO/IEC 27001: "Information technology -- Security techniques -- Information security management systems -- Requirements".

[i.61] ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security controls".

[i.62] ISO/IEC 27003: "Information technology -- Security techniques -- Information security management systems-- Guidance".

[i.63] ISO/IEC 27004: "Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation".

[i.64] ISO/IEC 27005: "Information technology -- Security techniques -- Information security risk management".

[i.65] ISO/IEC 27006: "Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems".

[i.66] ISO/IEC 27007: "Information technology -- Security techniques -- Guidelines for inf9ormation security management systems auditing".

[i.67] ISO/IEC 27010: "Information technology -- Security techniques -- Information security management for inter-sector and inter-organisational communications".

[i.68] ISO/IEC 27011: "Information technology -- Security techniques -- Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations".

[i.69] ISO/IEC 27013: "Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001".

[i.70] ISO/IEC 20000-1: "Information technology -- Service management -- Part 1: service management system requirements.

[i.71] ISO/IEC 27014: "Information technology -- Security techniques -- Governance of information security.

[i.72] ISO/IEC 27017: "Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services".

[i.73] Recommendation ITU-T X.1631: "Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services".

[i.74] ISO/IEC 27018: "Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".

[i.75] ISO 19005: "Document management -- Electronic document file format for long-term preservation".

[i.76] ISO 19005-2: "Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)".

[i.77] ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".

[i.78] ISO 23081-2: "Information and documentation -- Managing metadata for records -- Part 2: Conceptual and implementation issues".

[i.79] ISO/IEC JTC 1/SC 38: "Cloud Computing and Distributed Platforms".

[i.80] ISO/IEC 17021: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems".

[i.81] ISO/IEC TR 27008 (2011): "Information technology -- Security techniques -- Guidelines for auditors on information security controls".

[i.82] ISO/IEC TR 27015 (2012): "Information technology -- Security techniques -- Information security management guidelines for financial services".

[i.83] ISO/IEC TR 27016 (2014): "Information technology -- Security techniques -- Information security management -- Organizational economics".

[i.84] ISO/IEC TR 27019 (2013): "Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry".

[i.85] ISO/TR 15801 (2009): "Document management -- Information stored electronically -- Recommendations for trustworthiness and reliability".

[i.86] ISO/TR 17068 (2012): "Information and documentation - Trusted third party repository for digital records".

[i.87] ISO 23081-1 (2006): "Information and documentation -- Records management processes -- Metadata for records -- Part 1: Principles".

[i.88] ISO/DIS 17068: "Information and documentation - Trusted third party repository for digital records".

[i.89] ISO 14641-1 (2012): "Electronic archiving -- Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation".

[i.90] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.7] and the following apply:

blob: data object, manifested physically as a bytestream

NOTE: A blob object refers to a byte sequence that can be associated with additional information like the size and the type.

container: data object, which contains a sequence of data objects and related metadata and an optional manifest specifying the content, where the metadata can in particular comprise associated signatures, seals, time-stamps, evidence records, validation data (CRLs, OCSP responses) and validation reports as well as other application specific metadata

EXAMPLE: The format of a Container can be based on, ZIP [i.29] or XML [i.58] for example. ASiC according to [i.17] is an example of a Container based on ZIP [i.29].