ETSI TS 119 511 V1.1.1 (2019-06)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
trust service providers providing long-term preservation
of digital signatures or general data using
digital signature techniques

Reference

DTS/ESI-0019511

Keywords

electronic preservation, electronic signature,
trust 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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 and are a major cornerstone for electronic commerce.

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.2], 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.2] 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 is aiming to meet the general requirements of the international community to provide trust and confidence in preservation services which can be used to preserve the validity status of digital signatures or to provide a proof of existence of digital objects using digital signature techniques, including, amongst others, applicable requirements from Articles 34 and 40 of Regulation (EU) N 910/2014 [i.2] that establishes a legal framework for qualified preservation service for qualified electronic signatures and mutatis mutandis for qualified preservation service for qualified electronic seals.

1 Scope

The present document builds on the general policy requirements specified in ETSI EN 319 401 [1], specifies policy and security requirements for trust service providers providing long-term preservation of digital signatures and of general data, i.e. signed data or unsigned data, using digital signature techniques.

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

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.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.2].

The present document addresses two main cases:

1) The preservation **over long periods of time, using digital signature techniques**, of the **ability to validate a digital signature,** of the ability **to maintain its validity status** and of the ability **to get a proof of existence** of the associated signed data as they were at the time of the submission to the preservation service even if later the signing key becomes compromised, the certificate expires, or cryptographic attacks become feasible on the signature algorithm or the hash algorithm used in the submitted signature.

NOTE 1: A qualified preservation service for qualified electronic signatures or seals as per Regulation (EU) No 910/2014 [i.2] for which the status of the technical validity needs to be preserved, is covered in this case.

NOTE 2: The validity status of a signature means the status of the signature that will not change over time. Such a status may be valid (TOTAL_PASSED according to ETSI EN 319 102-1 [i.6]) or invalid (TOTAL_FAILED and certain cases for INDETERMINATE according to ETSI EN 319 102-1 [i.6]).

NOTE 3: "Digital signature techniques" designates techniques based on digital signatures, time-stamps or evidence records.

2) The provision of a proof of existence of digital objects, whether they are signed or not, **using digital signature techniques** (digital signatures, time-stamp tokens, evidence records, etc.).

NOTE 4: In this case, even if the main object to be preserved is a signature, it is treated in the same way as any other file.

NOTE 5: A proof of existence of digital object not using digital signature techniques is not in the scope of the present document.

The present document covers different strategies for the preservation service. The applicable requirements depend on the strategy chosen by the preservation service.

EXAMPLE 1: The preservation service can provide storage, no storage, or temporary storage.

EXAMPLE 2: The preservation service can receive the digital signature, the signed data, the revocation information or only hash values and evidences.

The present document identifies specific controls needed to address specific risks associated with preservation services.

The transformation of the original data into another data object with equivalent object content and semantic to avoid the risk that the original data object/viewer system is becoming obsolete is out of the scope of the present document.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

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

[2] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[3] ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".

[4] ISO/IEC 19790: "Information technology -- Security techniques -- Security requirements for cryptographic modules".

[5] FIPS PUB 140-2: "Security Requirements for Cryptographic Modules".

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] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.2] 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.3] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.4] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.5] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.6] 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.7] 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.8] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers".

[i.9] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.10] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.11] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.12] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[i.13] ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services".

[i.14] ISO/IEC 21320-1 (2015): "Information technology -- Document Container File -- Part 1: Core".

[i.15] ISO 14641-1:2018: "Electronic archiving -- Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation".

[i.16] ISO 14721:2012: "Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model".

[i.17] ISO 16363:2011: "Space data and information transfer systems -- Audit and certification of trustworthy digital repositories".

[i.18] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[i.19] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[i.20] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.21] IETF RFC 5280 (2008): Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.22] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".

[i.23] IETF RFC 6283 (2011): "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.24] IETF RFC 6960 (2013): "Online Certificate Status Protocol - OCSP".

[i.25] W3C Recommendation 26 November 2008: "Extensible Markup Language (XML) 1.0 (Fifth Edition)".

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

[i.26] BSI TR-03125-F: "Preservation of Evidence of Cryptographically signed Documents", Formats (TR-ESOR-F).

NOTE: Available at https://www.bsi.bund.de/EN/tr-esor_XAIP.

[i.27] BSI TR-03125-M.3: "Preservation of Evidence of Cryptographically signed Documents", Formats (TR-ESOR-M.3).

NOTE: Available at https://www.bsi.bund.de/EN/tr-esor.

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.4] and the following apply:

certificate status authority: authority providing certificate status information

EXAMPLE: The certificate status information can be provided using the Online Certificate Status Protocol (OCSP) [i.24] or in form of Certificate Revocation Lists (CRL) [i.21].

container: data object, which contains a set of data objects and optional additional information, which describes the contained data objects and optionally its content and its interrelationships

EXAMPLE: The format of a container can be based on, ZIP as defined in ISO/IEC 21320-1 [i.14] or XML [i.25]. ASiC [i.8] is an example of a container based on ZIP.

NOTE: Additional information may comprise associated digital signatures, time-stamps, evidence records, validation data (CRLs, OCSP responses) and validation reports.

data object: actual binary/octet data being operated on (e.g. transformed, digested, or signed) by an application and which may be associated with additional information like an identifier, the encoding, size or type

delta preservation object container: special preservation object container describing the difference to an already existing preservation object container

digital signature techniques: techniques based on digital signatures, time-stamps or evidence records

EU qualified time-stamping authority: qualified trust-service provider issuing qualified electronic time-stamps as laid down in Regulation (EU) 910/2014 [i.2]

evidence record: unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time

NOTE: See IETF RFC 4998 [i.20], IETF RFC 6283 [i.23] and ETSI TS 119 122-3 [i.7].

expected evidence duration: for a preservation service with temporary storage or without storage, duration during which the preservation service expects that the preservation evidence can be used to achieve the preservation goal

export-import package: information extracted from the preservation service including the submission data object (SubDO), the preservation evidence and preservation-related metadata, allowing another preservation service to import it in order to continue to achieve the preservation goal based on this information

long-term: time period during which technological changes may be a concern

EXAMPLE: Possible technological changes are obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises.

long-term preservation: extension of the validity status of a digital signature over long periods of time and/or extension of provision of proofs of existence of data over long periods of time, in spite of obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or of the loss of the ability to check the validity status of public key certificates

metadata: data about other data

NOTE: See ISO 14721:2012 [i.16].

notification protocol: protocol used by a preservation service to notify the preservation client

preservation client: component or a piece of software which interacts with a preservation service via the preservation protocol

preservation evidence: evidence produced by the preservation service which can be used to demonstrate that one or more preservation goals are met for a given preservation object

preservation evidence augmentation: addition of data to an existing preservation evidence to extend the validity period of that evidence

EXAMPLE: Adding a new time-stamp protecting additional validation data which can be used to validate a previous signature and/or time-stamp, and/or the hash of the protected data using a stronger hash algorithm.

preservation evidence policy: set of rules that specify the requirements and the internal process to generate or how to validate a preservation evidence

preservation evidence retention period: for a preservation service With Temporary Storage (WTS) the time period during which the evidences that are produced asynchronously can be retrieved from the preservation service

preservation goal: one of the following objectives achieved during the preservation time frame: extending over long periods of time the validity status of digital signatures, providing proofs of existence of data over long periods of time, or augmenting externally provided preservation evidences

NOTE: A preservation service can achieve one or more preservation goals.

preservation mechanism: mechanism used to preserve preservation objects and to maintain the validity of preservation evidences

NOTE: The present document only addresses preservation mechanisms based on digital signature techniques.

preservation interface: component implementing the preservation protocol on the side of the preservation service

preservation manifest: data object in a preservation object container referring to the preservation data objects or additional information and metadata in the preservation object container

EXAMPLE 1: Additional file in an ASiC-container according to ETSI EN 319 162-1 [i.8], clause A.7.

EXAMPLE 2: `versionManifest` in TR-ESOR-F [i.26].

EXAMPLE 3: An XML based manifest data element in an XML-based Preservation Object Container (POC).

preservation object: typed data object which is submitted to, processed by or retrieved from a preservation service

NOTE: This covers submission data objects, preservation object containers and preservation evidences.

preservation object container: container which contains a set of data objects and optionally related metadata providing information about the data objects and optionally preservation manifest(s) specifying its content and relationships

EXAMPLE 1: An ASiC-S or ASiC-E container is a Preservation Object Container that supports one or more signature and time assertion files each applicable to its own set of one or more files.

EXAMPLE 2: An OAIS Submission Information Packages is a Preservation Object Container.

preservation object identifier: unique identifier of a (set of) preservation object(s) submitted to a preservation service

preservation period: for a preservation service with storage, duration during which the preservation service preserves the submitted preservation objects and the associated evidences

NOTE: The submitted preservation objects can be updated during the preservation period.

preservation profile: uniquely identified set of implementation details pertinent to a preservation storage model and one or more preservation goals which specifies how preservation evidences are generated and validated

NOTE: See clause 4.3 of the present document and the description of a machine-readable version in ETSI TS 119 512 [i.13].

preservation protocol: protocol to communicate between the preservation service and a preservation client