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

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.