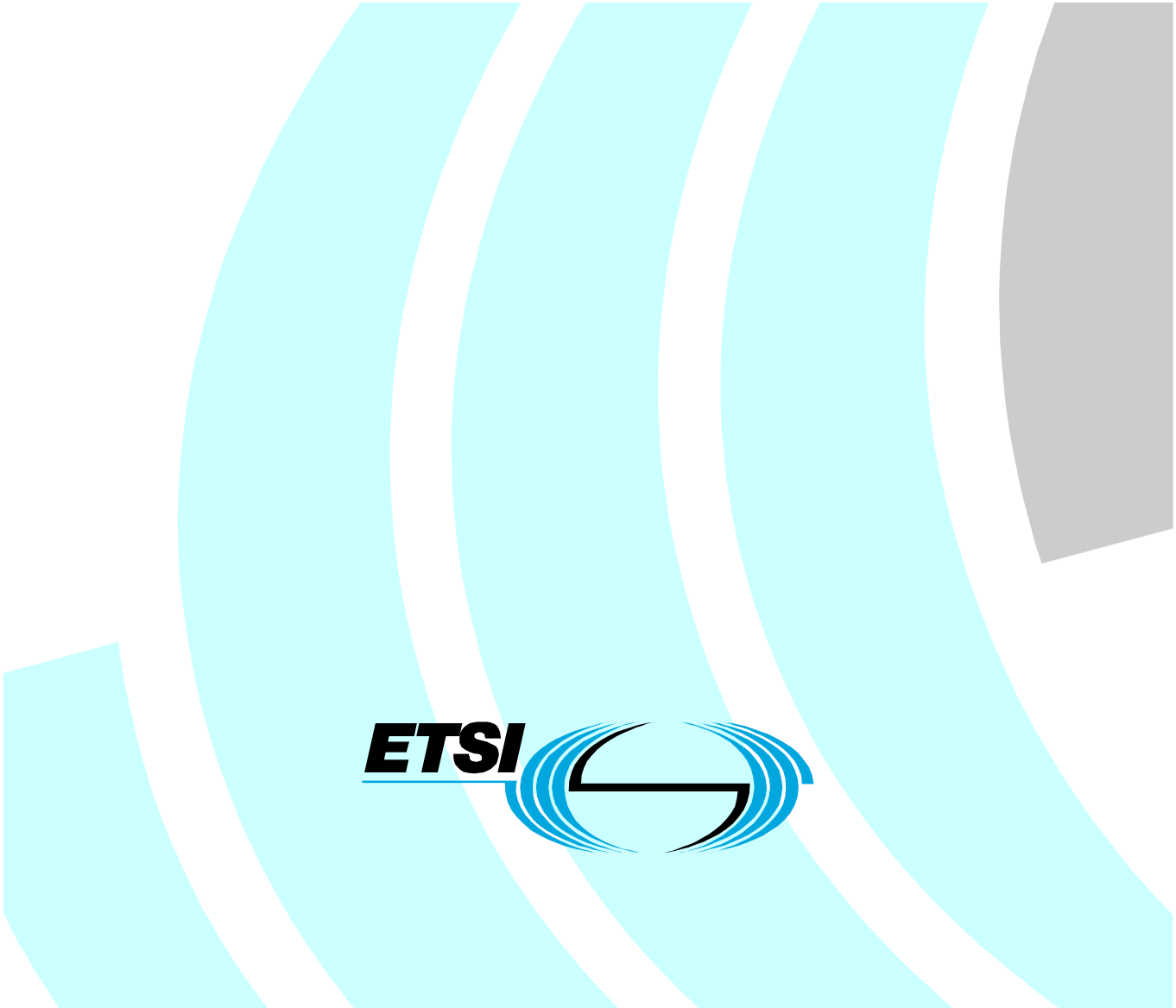
# ETSI TR 102 047 V1.1.1 (2004-02)

*Technical Report*

## International Harmonization of Electronic Signature Formats



Reference
DTR/ESI-000008

Keywords
e-commerce, electronic signature, digital, security

***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 (http://webapp.etsi.org/IPR/home.asp).

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.

# Foreword

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

# 1 Scope

The present document presents the results of ongoing work to harmonize existing ETSI technical specification on electronic signature formats (TS 101 733 [1] and TS 101 903 [2]) with other internationally recognized standards and related activities.

The aim of the present document is to identify the way forward to meet the requirements of European Electronic Signature Directive 1999/93/EC [5] for advanced electronic signatures in a manner which maximizes international interoperability.

# 2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI) ; Electronic Signature Formats".

[2] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

[3] IETF RFC 2630 (1999): "Cryptographic Message Syntax".

NOTE: Obsoletes RFC 3369.

[4] IETF RFC 3369: "Cryptographic Message Syntax".

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

[6] W3C Recommendation | IETF RFC 3275: XML-Signature Syntax and Processing.

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

NOTE: Equivalent to TS 101 733 v.1.2.2.

[8] W3C Note: XML Advanced Electronic Signatures (XAdES).

NOTE: Equivalent to ETSI TS 101 903 v1.1.1. http://www.w3.org/TR/2003/NOTE-XAdES-20030220/.

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 733 [1] and TS 101 903 [2] apply.

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| ASN.1 | Abstract Syntax Notation (number) 1 |
| CMS | Cryptographic Message Syntax |
| CRL | Certificate Revocation List |
| DSS | Digital Signature Services |
| DSS-TC | Digital Signature Services Technical Committee |
| EESSI | European Electronic Signature Standardization Initiative |
| IETF | Internet Engineering Task Force |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OCSP | Online Certificate Status Provider |

| | |
|---|---|
| TC | Technical Committee |
| W3C | World Wide Web Consortium |
| XAdES | XML Advanced Electronic Signatures |
| XML | eXtended Markup Language |
| XMLDSIG | XML-Signature Syntax and Processing |

# 4 Objective

The major objective of international harmonization on electronic signature formats is to maximize interoperability between electronic signatures in line with European electronic signature Directive [5] and other electronic signature systems.

# 5 International basis of European electronic signature formats

Recognizing the need to ensure that European electronic signatures are internationally harmonized the technical specifications developed in ETSI are based on existing internationally recognized standards as described in clause 5.1.

## 5.1 TS 101 733 and IETF RFC 2630/RFC 3369

IETF has specified a format for electronic signatures using the ASN.1 abstract syntax (RFC 2630 [3] now obsolete by RFC 3369 [4] "Cryptographic Message Syntax", CMS henceforward). This format defines the basic components for any electronic signature based on this syntax. It also presents mechanisms for incorporating additional information as required by the environment.

ETSI TS 101 733 [1]:

- Defines ASN.1 types for the additional attributes that have to be present in an electronic signature to remain valid over long periods, to satisfy common use cases requirements, and to be compliant with the European Directive.
- Proposes different advanced electronic signatures forms that satisfy the aforementioned requirements, based on the types defined.
- Presents an exhaustive rationale on each of the different new types.

TS 101 733 [1] specifies ASN.1 structures that can be added to the basic CMS signature, namely: indication of signing time, different time-stamps, indication of commitment gotten by the signer, indication of the signature place, identifier of a signature policy, indication of the signer role, countersignatures of a signature, and validation data, including references to certificates, CRLs or OCSP responses, or their corresponding values.

A new version of TS 101 733 [1] (v1.5.1) has been published in December 2003 taking into account external comments raised to ESI.

## 5.2 TS 101 903 and W3C XML signatures

W3C/IETF has specified a format for electronic signatures in XML (henceforward XMLDSIG). This format specifies the basic components of an XML electronic signature and defines mechanisms for incorporating additional information to the signature itself. TS 101 903 [2] XML Advanced Electronic Signatures (XAdES henceforward) was born as the counterpart of TS 101 733 [1] for XML. Specifically, TS 101 903 [2]:

- Shows a taxonomy of the additional elements (properties) that have to be present in an electronic signature to remain valid over long periods, to satisfy common use cases requirements, and to be compliant with the European Directive.
- Specifies XML schema definitions for new elements able to carry or to refer to the aforementioned properties.

- Specifies two ways for incorporating the qualifying information to XMLDSIG, namely either by direct incorporation of the qualifying information or using references to such information. Both ways make use of mechanisms defined in XMLDSIG.

- Proposes specific XML Advanced Electronic signatures that satisfy the aforementioned requirements by combining the defined elements.

As its ASN.1 counterpart, TS 101 903 [2] define XML structures able to contain similar information to that mentioned in the previous section.

TS 101 903 [2] is currently being reviewed in the light of external comments appeared after its publication and the first XAdES interoperability event organized by ETSI. The completion of the new version of TS 101 903 [2] is scheduled for the end of March of 2004.

# 6 Further harmonization activities

## 6.1 RFC 3126

Members of the ETSI TC ESI have fed the TS 101 733 [1] into the Internet Engineering Task Force as a Informational specification which is technically identical to TS 101 733 [1] v1.2.2. This has resulted in the work of ETSI being visible internationally and has resulting in the use of the same technique outside Europe, maximizing international interoperability.

Recently, TS 101 733 [1] has been updated (v1.5.1) to address a number of issues coming from different external sources in implementing the earlier version. It is recommended that IETF are requested to publish a new Informational RFC to replace RFC 3126 [7] which is equivalent to the latest version of TS 101 733 [1] (v1.5.1).

## 6.2 W3C Note

Once the TS 101 903 [2] was issued, a W3C (World Wide Web Consortium) Note [8] was produced as a way of attracting the attention of agents outside Europe. Currently, more and more notifications of developments of XAdES are being known.

The ETSI TC ESI is updating TS 101 903 [2] from comments coming from different sources: standardization organizations outside Europe, implementers, etc. It is recommended that the W3C Note is updated to reflect these changes.

In addition, and within the context of a XAdES interoperability event organized by ETSI in November 2003, W3C was contacted to discuss about which could be the best way for proceeding forward with XAdES within W3C. Currently, the first contacts between ETSI and W3C are taking place with the objective of setting up a Joint Working Group that would deal with the progress of XAdES and potentially upcoming standards in the area.

## 6.3 OASIS DSS

In 2002 OASIS (Organization for the Advancement of Structured Information Standards), set up the Digital Signature Services Technical Committee (DSS-TC), whose main objectives are:

- To "develop a protocol for a digital signature creation web service. Providing digital signatures via such a web service facilitates policy-based control of the provision of the signatures".

- To "develop a protocol for a centralized digital signature verification web service that can verify signatures in relation to a given policy set".

- To "develop an XML-based protocol to produce cryptographic time stamps that can be used for determining whether or not a signature was created within the associated key's validity period or before revocation".

- To specify a XML time-stamp token format.

The TC has already drafted the DSS Core Protocol, supporting both requests and responses for both Signing and Signature Validation operations.

The TC has also drafted a first version of an XML time-stamp token.

Currently, the TC has also identified a number of profiles for the DSS Core Protocol, each of them will be designed to satisfy specific well-known requirements in different domains.

One of the profiles being defined deals with XAdES signatures specified in TS 101 903 [2]. This profile will define a protocol able to cover the lifecycle of a XAdES signature. This means that it will provide with operations for:

- Requesting the creation of a XAdES signature, and responding to this request.
- Requesting the validation of the formerly created XAdES signature, and responding to this request, which can include the incorporation of validation data to the signature (time-stamp on the signature, references to certificates, CRLs, etc).
- Requesting incorporation of additional properties for getting archival forms of XAdES, and responding to these requests.
- Requesting re-validation for arbitration purposes, and responding to these requests.

In addition, up to two other identified profiles (EPM and German Signature profile) have shown certain overlap with XAdES profile such as are using time-stamping for archival, as they incorporate in their scenarios the usage of certain XAdES forms and/or properties.

This work will continue during the first half of year 2004, so that it will eventually end with a DSS-XAdES profile.

Two members of the ETSI TC ESI joined this TC since its birth. Currently both of them share the responsibility of co-chairing the TC and leading the works of XAdES profiling group.

# 7 Recommendations

The ETSI specifications on electronic signature formats (TS 101 733 [1] and TS 101 903 [2]) are very closely harmonized with other similar international standardization. The specifications were based on existing international specifications for electronic signature formats (RFC 2630 [3] / RFC 3369 [4] and RFC 3275 [6]) and have been feed back for publication within the relevant groups.

It is recommended that the revisions to TS 101 733 [1] and TS 101 903 [2] are also fed back into the relevant groups (IETF and W3C) for publication in those for a to maintain continued harmonization.

It is also recommended that close links are maintained with the OASIS DSS technical committee to ensure that their work on web services continues to incorporate support for TS 101 903 [2].

Finally, it is recommended that the ETSI TC ESI maintain close ties with the W3C and if possible set up a joint group to continue work on electronic signature formats.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | February 2004 | Publication |
| | | |
| | | |
| | | |
| | | |