ETSI TR 102 047 V1.2.1 (2005-03)

Technical Report

International Harmonization of Electronic Signature Formats

Reference

RTR/ESI-000028

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2005.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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 specifications 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 Directive 1999/93/EC [4] 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 3369: "Cryptographic Message Syntax".

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

[5] W3C Recommendation/IETF RFC 3275: "XML-Signature Syntax and Processing".

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

NOTE: Equivalent to TS 101 733.

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

NOTE 1: See. http://www.w3.org/TR/2003/NOTE-XAdES-20030220/.

NOTE 2: Equivalent to TS 101 903.

[8] oasis-dss-1.0-core-spec-cd-02: "Digital Signature Service Core Protocols, Elements, and Bindings".

[9] ETSI TR 102 047: "International Harmonization of Electronic Signature Formats".

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
DTD	Document Type Definition
EPM	Electronic Post Mark

IETF	Internet Engineering Task Force
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Provider
TC	Technical Committee
URI	Uniform Resource Identifier
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 1999/93/EC [4] 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

IETF has specified a format for electronic signatures using the ASN.1 abstract syntax (RFC 3369 [3]). 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.

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] 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 XML Signature Syntax and Processing (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) 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 clause 5.1.

TS 101 903 [2] has been reviewed in the light of external comments and the first XAdES interoperability event organized by ETSI. The new version of TS 101 903 [2] was publish in first half of 2004.

6 Further harmonization activities

6.1 IETF RFC 3126

Members of the ETSI TC ESI have fed the TS 101 733 [1] into the Internet Engineering Task Force (IETF) as an informational specification which is technically identical to TS 101 733 [1]. 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 to address a number of issues coming from different external sources in implementing the earlier version. Text for an Internet Draft to replace RFC 3126 [6] in line with the new version TS 101 733 [1] has been produced. However, at the time the present document was produced progress of this Internet Draft has been halted pending resolution of IPR issues following changes in the IETF IPR rules.

6.2 W3C Note and joint working group

Once the TS 101 903 [2] was issued, a W3C Note [7] was produced as a way of attracting the attention of agents outside Europe. Currently, more and more implementations of XAdES are becoming known.

The ETSI TC ESI has updated TS 101 903 [2] with comments coming from different sources including standardization organizations outside Europe, implementers, etc. Discussions have been held with W3C concerning updating the existing W3C as well as other activities on XML signatures. As a result it has been proposed that W3C and ETSI set up a joint activity on XML signatures to work together on advanced XML signatures.

6.3 OASIS Digital Signature Services (DSS)

In 2002 OASIS (Organization for the Advancement of Structured Information Standards), set up the Digital Signature Services Technical Committee (DSS-TC). The mandate of the DSS-TC is the development of techniques to support the processing of digital signatures. This mandate includes defining an interface for requesting that a web service produce and/or verify a digital signature on a given piece of data and techniques for proving that a signature was created within its key validity period.

The TC is developing:

- 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.

- A digital signature verification web service that can verify signatures in relation to a given policy set.

- 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. The TC will also develop an XML format for cryptographic time-stamps.

- A set of profiles of the aforementioned protocols. These profiles will define specific uses of the general protocols to address specific applications.

The DSS specifications consist of a specification which defines the Core Protocol, elements and bindings, including protocols for creation and verification of signatures and an XML structure for time-stamps. A number of profiles have been defined which selects options within the Core and adds additional elements necessary to support particular use cases. Profiles have been drafted for:

- Time-stamping services;
- Asynchronous operation;
- Code signing;
- Entity seal;
- Electronic Post Mark (EPM);
- German signature law;
- Policy wise operation;
- XML Advanced Electronic Signature (XAdES) (as in TS 101 903 [2]).

The TC has close to agreeing a set of Committee Drafts for the DSS Core Protocol and the above profiles.

Profiles are also being developed or are planned for:

- Signature gateway;
- Court filing;
- Electronic notaries;
- Web security services.

The use of the OASIS time-stamping protocol profile and XML token format is being incorporated within the ANSI standard X9.95 for "Trusted Time Stamp Management and Security".

XAdES profile supports the creation and validation of signatures as in TS 101 903 [2]. This profile defines 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.

Having agreed the Committee Drafts, it is planned to produce trial implementations to test interoperability before the documents are formally put out for public review and progression to an OASIS standard.

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.

Further technical information about DSS is provided in annex A.

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 3369 [3] and RFC 3275 [5]) and have been feed back for publication within the relevant groups.

It is recommended that work continues to feed the revisions to TS 101 733 [1] and TS 101 903 [2] 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.

Annex A: Further technical details of OASIS DSS

This annex summarizes the technical details for most relevant activities held in the OASIS Digital Signature Services Technical Committee (DSS-TC).

First of all, details on the current situation of the Core Protocol will be given.

Afterwards, details on the current situation of the profile written for the protocol able to request generation and verification of XAdES and TS 101 733 [1] electronic signatures, will be given.

The former will be followed by details on the rest of profiles.

Afterwards the document presents some information on liaisons established with other standardization groups.

Finally, some hints on future activities will be given.

A.1 OASIS DSS Core Protocol

At present, the latest version of the Core Protocol, defined in the document **"Digital Signature Service Core Protocols, Elements, and Bindings" [**8**]** is version 30.

Since that the version 26 was approved as Committee Draft, the most relevant improvements are:

1) Capability for including the schema (previous versions only managed DTDs) of the signed documents whose signature has to be verified for making apparent the ID type attributes whose name is not Id, ID, etc.

2) Text and elements added for introducing capabilities for dealing with <ds:Manifest> processing.

3) Text clarifying the semantics of the <dss:ReturnSigningTime> optional input and the corresponding <dss:SigningTime> optional output*: "This output typically gives the client access to a time value carried within a signature attribute or a signature timestamp, or within a timestamp token if the signature itself is a timestamp".*

4) Modification of <dss:ClaimedIdentity> (element indicating *"the identity of the client who is making a request"*). Added element able to contain *"Information supporting the name"* ,like SAML assertions, X509 certificate, etc.

At the time the present document is written, there is a ballot opened for progressing this version 30 to the Committee Draft Status.

A.2 OASIS DSS XAdES-related protocols

Since the last report [9] two new versions of the document **"XAdES Profiles of the OASIS Digital Signature Service"** have been generated. The latest version is version number 6.

At present the document contains:

1) An abstract profile (i.e. a profile that may not be instantiated by providers) for two protocols. One for requesting generation XML or TS 101 733 [1] advanced electronic signatures, and other for requesting verification (and optionally update –i.e. addition of unsigned properties) of the aforementioned signatures.

2) Two concrete profiles (i.e. profiles that may be implemented and instantiated by providers):

   a) The first one contains two protocols. One for requesting TS 101 733 [1] advanced electronic signatures generation and another for requesting verification (and optionally update) of the aforementioned signatures.

b) The second one contains also two protocols. One for requesting XAdES electronic signatures generation and another for requesting verification (and optionally update) of the aforementioned signatures.

The two concrete profiles incorporate similar features for both types of signatures TS 101 733 [1] and XAdES, except for the fact that XAdES allows incorporate time-stamps on individual objects to be signed, whereas TS 101 733 [1] does not support this distinction (due to the CMS format).

Below follows the most relevant features:

1) The **generation protocols** allow request of certain signed signatures on individual basis. This means that the client may request to the server the incorporation of one or several of the following properties: `SigningTime,CommitmentTypeIndication, SignatureProductionPlace, SignerRole, DataObjectFormat` and `DataObjectTimeStamp.`

2) In addition, the concrete profile for requesting generation of XAdES signatures, allows requesting `IndividualDataObjectTimeStamp`.

3) When requesting incorporation of signed properties, the **generation profiles** allow the client to pass to the server the values of the following properties: `CommitmentTypeIndication, SignerRole, IndividualDataObjectTimeStamp` and `DataObjectFormat`. The request message will incorporate their values as XML elements (in the XAdES concrete profile) or as binary values (as defined in TS 101 733 [1]) base-64 encoded and encapsulated in XML elements (in the TS 101 733 [1] concrete profile).

4) For incorporation of the rest of properties, the generation protocols work on a signature form basis. This means that for requesting incorporation of `SignaturePolicyIdentifier`, or the `SignatureTimeStamp`, the client will incorporate a **URI** that identifies the XAdES or the TS 101 733 [1] signature form. The two concrete profiles allow to manage **all the forms specified in the latest versions of XAdES and TS 101 733 [1].**

5) The **verification protocols** have as input XAdES or TS 101 733 [1] and their corresponding signed documents. They allow to request the server the verification of the signature and the incorporation of additional unsigned properties so that the server may return to the client a more evolved form (a XAdES-T could be send to the server, and get a XAdES-C in response or even a XAdES-X). In this way, the service defined goes beyond the verification features and incorporates also updating features.

This profile, along with other profiles whose details will be given in the next clause is, at the moment when the present document is written, being voted for being progressed to Committee Draft status.

History

Document history		
V1.1.1	February 2004	Publication
V1.2.1	March 2005	Publication