ETSI TS 101 733 V1.7.4 (2008-07)

Technical Specification

Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

Reference
RTS/ESI-000061

Keywords
e-commerce, electronic signature, 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

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

Introduction

Electronic commerce is emerging as the future way of doing business between companies across local, wide area and global networks. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is, therefore, important that companies using this electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect the electronic signature is an important security component that can be used to protect information and provide trust in electronic business.

The present document is intended to cover electronic signatures for various types of transactions, including business transactions (e.g. purchase requisition, contract, and invoice applications) where long-term validity is important. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (i.e. repudiates; see ISO/IEC 10181-5 [i.1]) the validity of the signature.

Thus, the present document can be used for any transaction between an individual and a company, between two companies, between an individual and a governmental body, etc. The present document is independent of any environment; it can be applied to any environment, e.g. smart cards, GSM SIM cards, special programs for electronic signatures, etc.

The European Directive on a community framework for Electronic Signatures defines an electronic signature as: "Data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication".

An electronic signature, as used in the present document, is a form of advanced electronic signature as defined in the Directive.

1 Scope

The scope of the present document covers electronic signature formats only, previous versions of the present document covered both Electronic Signature Formats and Electronic Signature Policies. The aspects of Electronic Signature Policies covered by previous versions of the present document are now defined in TR 102 272 [i.2].

The present document defines a number of electronic signature formats, including electronic signatures that can remain valid over long periods. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the electronic signature.

The present document specifies use of Trusted Service Providers (e.g. Time-Stamping Authorities) and the data that needs to be archived (e.g. cross certificates and revocation lists) to meet the requirements of long-term electronic signatures.

An electronic signature, as defined by the present document, can be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later.

The present document includes the concept of signature policies that can be used to establish technical consistency when validating electronic signatures, but it does not mandate their use.

The present document is based on the use of public key cryptography to produce digital signatures, supported by public key certificates. The present document also specifies the use of time-stamping and time-marking services to prove the validity of a signature long after the normal lifetime of critical elements of an electronic signature. The present document also, as an option, defines ways to provide very long-term protection against key compromise or weakened algorithms.

The present document builds on existing standards that are widely adopted. These include:

- RFC 3852 [4]: "Cryptographic Message Syntax (CMS)";
- ISO/IEC 9594-8/ITU-T Recommendation X.509 [1]: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks";
- RFC 3280 [2]: "Internet X.509 Public Key Infrastructure (PKIX) Certificate and Certificate Revocation List (CRL) Profile";
- RFC 3161 [7]: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

NOTE: See clause 2 for a full set of references.

The present document describes formats for advanced electronic signatures using ASN.1 (Abstract Syntax Notation 1). These formats are based on CMS (Cryptographic Message Syntax) defined in RFC 3852 [4]. These electronic signatures are thus called CAdES, for "CMS Advanced Electronic Signatures".

Another document, TS 101 903 [i.3], describes formats for XML Advanced Electronic Signatures (XAdES) built on XMLDSIG.

In addition, the present document identifies other documents that define formats for Public Key Certificates, Attribute Certificates, and Certificate Revocation Lists and supporting protocols, including protocols for use by trusted third parties to support the operation of electronic signature creation and validation.

Informative annexes include:

- illustrations of extended forms of Electronic Signature formats that protect against various vulnerabilities and examples of validation processes (annex B);
- descriptions and explanations of some of the concepts used in the present document. giving a rational for normative parts of the present document (annex C);
- information on protocols to interoperate with Trusted Service Providers (annex D);
- guidance on naming (annex E);

- an example structured content and MIME (annex F);
- the relationship between the present document and the directive on electronic signature and associated standardization initiatives (annex G);
- APIs to support the generation and verification of electronic signatures (annex H);
- cryptographic algorithms that may be used (annex I); and
- naming schemes (annex J).

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ITU-T Recommendation X.509 (2000) / ISO/IEC 9594-8 (2001): "Information technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate frameworks".

[2] IETF RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[3] IETF RFC 2560 (1999): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[4] IETF RFC 3852 (2004): "Cryptographic Message Syntax (CMS)".

[5] IETF RFC 2634 (1999): "Enhanced Security Services for S/MIME".

[6] IETF RFC 2045 (1996): "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[7] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[8] ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[9] ITU-T Recommendation X.501 (2000) / ISO/IEC 9594-1 (2001): "Information technology - Open Systems Interconnection - The Directory: Models".

[10] IETF RFC 3370 (2002): "Cryptographic Message Syntax (CMS) Algorithms".

[11] ITU-T Recommendation F.1: "Operational provisions for the international public telegram service".

[12] ITU-T Recommendation X.500: "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".

[13] IETF RFC 3281 (2002): "An Internet Attribute Certificate Profile for Authorization".

[14] ITU-T Recommendation X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)".

NOTE: ITU-T Recommendation X.208 has been withdrawn on 30 October 2002 as it has been superseded by ITU-T Recommendations X.680-683. All known defects in X.208 have been corrected in ITU-T Recommendations X.680-683 (1993) further revised in 1997 and 2002. However, the reference is kept in the current to ensure compatibility with RFC 3852 [4].

[15] IETF RFC 5035 (2007): "ESS Update: Adding CertID Algorithm Agility"..

[16] ITU-T Recommendation X.690 (2002): "Information technology ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

NOTE: This Internet Draft is due to be shortly published as an Internet RFC. The present document will be re-issued with the RFC reference when it becomes available.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ISO/IEC 10181-5 (April 1997): "Security Frameworks in Open Systems. Non-Repudiation Framework".

[i.2] ETSI TR 102 272: "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies".

[i.3] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

[i.4] ISO 7498-2 (1989): "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

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

[i.6] ISO/IEC 13888-1 (2004): "IT security techniques - Non-repudiation - Part 1: General".

[i.7] ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

[i.8] IETF RFC 3125 (2000): "Electronic Signature Policies".

[i.9] ETSI TS 101 861: "Time stamping profile".

[i.10] IETF RFC 3494 (2003): "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2".

[i.11] IETF RFC 4523 (2006): " Lightweight Directory Access Protocol (LDAP). Schema Definitions for X.509 Certificates".

[i.12] IETF RFC 4210 (2005): "Internet X.509 Public Key Infrastructure Certificate Management Protocols".

[i.13] IETF RFC 3851: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification".

[i.14] IETF RFC 2743 (2000): "Generic Security Service Application Program Interface Version 2, Update 1".

[i.15] IETF RFC 2479 (1998): "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)".

[i.16] ISO/IEC 10118-1: "Information technology - Security techniques - Hash-functions - Part 1: General".

[i.17] ISO/IEC 10118-2: "Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher algorithm".

[i.18] ISO/IEC 10118-3: "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions".

[i.19] ISO/IEC 10118-4 (1998): "Information technology - Security techniques - Hash-functions - Part 4: Hash-functions using modular arithmetic".

[i.20] ANSI X9.30-2 (1997): "Public Key Cryptography for the Financial Services Industry - Part 2: The Secure Hash Algorithm (SHA-1)".

[i.21] ANSI X9.31-2 (1996): "Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry - Part 2: Hash Algorithms".

[i.22] IETF RFC 2437 (1998): "PKCS #1: RSA Cryptography Specifications Version 2.0".

[i.23] IEEE 1363 (2000): "Standard Specifications for Public-Key Cryptography".

[i.24] ISO/IEC 9796: "Information technology - Security techniques - Digital signature scheme giving message recovery".

[i.25] ISO/IEC 9796-2: "Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms".

[i.26] ISO/IEC 9796-4: "Digital signature schemes giving message recovery - Part 4: Discrete logarithm based mechanisms".

[i.27] ISO/IEC 14888-1 (1998): "Information technology - Security techniques - Digital signatures with appendix - Part 1: General".

[i.28] ISO/IEC 14888-2 (1999): "Information technology - Security techniques - Digital signatures with appendix - Part 2: Identity- based mechanisms".

[i.29] ISO/IEC 14888-3 (1998): "Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms".

[i.30] ISO/IEC 15946-3 (2002): "Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 3: Key establishment".

[i.31] ANSI X9.30.1 (1997): "Public Key Cryptography Using Irreversible Algorithms - Part 1: The Digital Signature Algorithm".

[i.32] ANSI X9.62 (2005): "Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA)".

[i.33] IETF RFC 2068: "Hypertext Transfer Protocol - HTTP/1.1".

[i.34] IETF RFC 4346 (2006): "The TLS Protocol Version 1.1".

[i.35] IETF RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

[i.36] IETF RFC 3369: "Cryptographic Message Syntax (CMS)".

[i.37] ISO/IEC 15946-2: "Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures".

[i.38] CWA 14171:2004: "General guidelines for electronic signature verification".

[i.39] FIPS Pub 180-2: "Secure Hash Standard (SHS)".

[i.40] ANSI X9.31 (1998): "Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)".

[i.41] ANSI X9.31-1: "American National Standard, Public-Key Cryptography Using Reversible Algorithms for the Financial Services Industry".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

arbitrator: arbitrator entity may be used to arbitrate a dispute between a signer and verifier when there is a disagreement on the validity of a digital signature

Attribute Authority (AA): authority that assigns privileges by issuing attribute certificates

authority certificate: certificate issued to an authority (e.g. either to a certification authority or an attribute authority)

Attribute Authority Revocation List (AARL): revocation list containing a list of references to certificates issued to AAs that are no longer considered valid by the issuing authority

Attribute Certificate Revocation List (ACRL): revocation list containing a list of references to attribute certificates that are no longer considered valid by the issuing authority

Certification Authority Revocation List (CARL): revocation list containing a list of public key certificates issued to certification authorities that are no longer considered valid by the certificate issuer

Certification Authority (CA): authority trusted by one or more users to create and assign public key certificates; optionally, the certification authority may create the users' keys

NOTE: See ITU-T Recommendation X.509 [1].

Certificate Revocation List (CRL): signed list indicating a set of public key certificates that are no longer considered valid by the certificate issuer

digital signature: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

NOTE: See ISO 7498-2 [i.4].

electronic signature: data in electronic form that is attached to or logically associated with other electronic data and that serves as a method of authentication

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

extended electronic signatures: electronic signatures enhanced by complementing the baseline requirements with additional data, such as time-stamp tokens and certificate revocation data, to address commonly recognized threats

Explicit Policy-based Electronic Signature (EPES): electronic signature where the signature policy that shall be used to validate it is explicitly specified

grace period: time period that permits the certificate revocation information to propagate through the revocation process to relying parties

initial verification: process performed by a verifier done after an electronic signature is generated in order to capture additional information that could make it valid for long-term verification

Public Key Certificate (PKC): public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority that issued it

NOTE: See ITU-T Recommendation X.509 [1].

Rivest-Shamir-Adleman (RSA): asymmetric cryptography algorithm based on the difficulty to factor very large numbers using a key pair: a private key and a public key

signature policy: set of rules for the creation and validation of an electronic signature that defines the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need, and under which the signature can be determined to be valid

signature policy issuer: entity that defines and issues a signature policy

signature validation policy: part of the signature policy that specifies the technical requirements on the signer in creating a signature and verifier when validating a signature

signer: entity that creates an electronic signature

subsequent verification: process performed by a verifier to assess the signature validity

NOTE: Subsequent verification may be done even years after the electronic signature was produced by the signer and completed by the initial verification, and it might not need to capture more data than those captured at the time of initial verification.

time-stamp token: data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time

time-mark: information in an audit trail from a Trusted Service Provider that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time

time-marking authority: trusted third party that creates records in an audit trail in order to indicate that a datum existed before a particular point in time

Time-Stamping Authority (TSA): trusted third party that creates time-stamp tokens in order to indicate that a datum existed at a particular point in time

Time-Stamping Unit (TSU): set of hardware and software that is managed as a unit and has a single time-stamp token signing key active at a time

Trusted Service Provider (TSP): entity that helps to build trust relationships by making available or providing some information upon request

validation data: additional data that may be used by a verifier of electronic signatures to determine that the signature is valid

valid electronic signature: electronic signature that passes validation

verifier: entity that verifies evidence

NOTE 1: See ISO/IEC 13888-1 [i.6].

NOTE 2: Within the context of the present document, this is an entity that validates an electronic signature.