SLOVENSKI STANDARD
SIST-TS ETSI/TS 101 733 V1.2.1:2005

01-maj-2005

Formati elektronskega podpisa

Electronic signature formats

Ta slovenski standard je istoveten z: **TS 101 733 Version 1.2.2**

ICS:

35.040	Nabori znakov in kodiranje informacij	Character sets and information coding

SIST-TS ETSI/TS 101 733 V1.2.1:2005 **en**

ETSI TS 101 733 V1.2.2 (2000-12)

Technical Specification

Electronic signature formats

Reference
DTS/SEC-004001

Keywords
IP, 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://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

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://www.etsi.org/ipr).

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 Security (SEC).

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). 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.

An electronic signature produced in accordance with the present document provides evidence that can be processed to get confidence that some commitment has been explicitly endorsed under a Signature policy, at a given time, by a signer under an identifier, e.g. a name or a pseudonym, and optionally a role.

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 current document is a form of advanced electronic signature as defined in the Directive.

1 Scope

The present document defines an electronic signature that remains 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 signature.

The present document specifies use of trusted service providers (e.g. TimeStamping 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 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 uses a signature policy, referenced by the signer, as the basis for establishing the validity of an electronic signature.

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 timestamping services to prove the validity of a signature long after the normal lifetime of critical elements of an electronic signature and to support non-repudiation. It also, as an option, defines the use of additional timestamps to provide very long-term protection against key compromise or weakened algorithms.

The present document builds on existing standards that are widely adopted. This includes:

- RFC 2630 [8] "Cryptographic Message Syntax (CMS)";
- ITU-T Recommendation X.509 [1]: "Information technology - Open Systems Interconnection - The Directory: Authentication framework";
- RFC 2459 [6] "Internet X.509 [23] Public Key Infrastructure (PKIX) Certificate and CRL Profile";
- IETF Internet Draft Time Stamp Protocol (TPS) (to be published) (see bibliography).

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

The present document includes:

- format of Electronic Signature tokens;
- format of Signature Policies.

In addition, the present document identifies other documents that define format for Public Key Certificates, Attribute Certificates, Certificate Revocation Lists and supporting protocols. Including, protocols for use of trusted third parties to support the operation of electronic signature creation and validation, as well as the management of certificates used to support electronic signatures.

Informative annexes, describe:

- an example structured content;
- the relationship between the present document and the directive on electronic signature and associated standardization initiatives;
- APIs to support the generation and the verification of electronic signatures;
- cryptographic algorithms that may be used;
- guidance on naming.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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.
- For a non-specific reference, the latest version applies.

[1] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Authentication framework".

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

[3] ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1: "Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[4] ITU-T Recommendation F.1 (1998): "Operational provisions for the international public telegram service".

[5] RFC 1777 (1995): "Lightweight Directory Access Protocol".

[6] RFC 2459 (1999): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

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

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

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

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

[11] ISO/IEC 13888-1 (1997): "Information technology - Security techniques - Non-repudiation - Part 1: General".

[12] ITU-T Recommendation X.400 (1996): "Message handling system and service overview".

[13] ITU-T Recommendation X.500 (1997): "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".

[14] ITU-T Recommendation X.501 (1997): "Information technology - Open Systems Interconnection - The Directory: Models".

[15] ITU-T Recommendation X.520 (1997): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[16] RFC 2559 (1999): "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2".

[17] RFC 2587 (1999): "Internet X.509 Public Key Infrastructure LDAPv2 Schema".

[18] RFC 2510 (1999): "Internet X.509 Public Key Infrastructure Certificate Management Protocols".

[19] RFC 2450 (1998): "Proposed TLA and NLA Assignment Rules".

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

[21] RFC 2078 (1997): "Generic Security Service Application Program Interface, Version 2".

[22] RFC 2511 (1999): "Internet X.509 Certificate Request Message Format".

[23] ITU-T Recommendation X.509 (2000): "Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks".

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

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 which assigns privileges by issuing attribute certificates

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

Attribute Authority Revocation List (AARL): references to attribute certificates issued to AAs, that are no longer considered valid by the issuing authority

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

Certification Authority (CA): authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys (ITU-T Recommendation X.509 [1])

Certificate Revocation List (CRL): signed list indicating a set of 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 (ISO 7498-2 [10])

public key certificate: public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it (ITU-T Recommendation X.509 [1])

signature policy: set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid

signature policy issuer: entity that defines the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need

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

signer: entity that creates an electronic signature

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

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

valid electronic signature: electronic signature which passes validation according to a signature validation policy

verifier: entity that verifies an evidence (ISO/IEC 13888-1 [11])

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

3.2 Abbreviations

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

AA	Attribute Authority
API	Application Program Interface
ARL	Authority Revocation List
ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
DSA	Digital Signature Algorithm (see annex E on crytpographic algorithms)
EDIFACT	Electronic Data Interchange for Administration, Commerce And Transport
ES	Electronic Signature
ES-A	ES with Archive Validation Data
ES-C	ES with Complete validation data
ESS	Enhanced Security Services (enhances CMS)
ES-T	ES with Timestamp
ES-X	ES with eXtended validation data
MIME	Multipurpose Internet Mail Extensions
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Internet X.509 [23] Public Key Infrastructure
SHA-1	Secure Hash Algorithm 1 (see annex E on crytpographic algorithms)
TSA	TimeStamping Authority
TSP	Trusted Service Provider
XML	eXtended Mark up Language

4 Overview

4.1 Major Parties

The following are the major parties involved in a business transaction supported by electronic signatures as defined in the present document:

- the Signer;
- the Verifier;
- Trusted Service Providers (TSP);
- the Arbitrator.

The **Signer** is the entity that initially creates the electronic signature. When the signer digitally signs over data using the prescribed format, this represents a commitment on behalf of the signing entity to the data being signed.

The **Verifier** is the entity that validates the electronic signature, it may be a single entity or multiple entities.

The **Trusted Service Providers** (TSPs) are one or more entities that help to build trust relationships between the signer and verifier. They support the signer and verifier by means of supporting services including: user certificates, cross-certificates, timestamping tokens, CRLs, ARLs, OCSP responses. The following TSPs are used to support the functions defined in the present document:

- Certification Authorities;
- Registration Authorities;

- Repository Authorities (e.g. a Directory);
- TimeStamping Authorities;
- Signature Policy Issuers.

Certification Authorities provide users with public key certificates.

Registration Authorities allow the identification and registration of entities before a CA generates certificates.

Repository Authorities publish CRLs issued by CAs, signature policies issued by Signature Policy Issuers and optionally public key certificates.

TimeStamping Authorities attest that some data was formed before a given trusted time.

Signature Policy Issuers define the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need. The procedural requirements may include requirements concerning the security evaluation of the products used for signature creation and validation.

In some cases the following additional TSPs are needed:

- Attribute Authorities.

Attributes Authorities provide users with attributes linked to public key certificates.

An **Arbitrator** is an entity that arbitrates in disputes between a signer and a verifier.

4.2 Electronic Signatures and Validation Data

Validation of an electronic signature in accordance with the present document requires:

- The electronic signature; this includes:
  - the signature policy;
  - the signed user data;
  - the digital signature;
  - other signed attributes provided by the signer.
- Validation data which is the additional data needed to validate the electronic signature; this includes:
  - certificates;
  - revocation status information;
  - trusted time-stamps from Trusted Service Providers (TSPs).

The **signature policy** specifies the technical and procedural requirements on signature creation and validation in order to meet a particular business need. A given legal/contractual context may recognize a particular signature policy as meeting its requirements. For example: a specific signature policy may be recognized by court of law as meeting the requirements of the European Directive for electronic commerce. A signature policy may be written using a formal notation like ASN.1 (see clause 11.1) or in an informal free text form provided the rules of the policy are clearly identified. However, for a given signature policy there shall be one definitive form which has a unique binary encoded value.

Signed user data is the user's data that is signed.

The **Digital Signature** is a digital signature applied over the following attributes provided by the signer:

- hash of the user data;
- signature Policy Identifier;
- other signed attributes.

The **other signed attributes** include any additional information which shall be signed to conform to the signature policy or the present document (e.g. signing time).

According to the requirements of a specific signature policy in use, various **Validation Data** shall be collected and attached to or associated with the signature structure by the signer and/or the verifier. The validation data includes CA certificates as well as revocation status information in the form of certificate revocation lists (CRLs) or certificate status information provided by an on-line service. Additional data also includes timestamps and other time related data used to provide evidence of the timing of given events. It is required, as a minimum, that either the signer or verifier obtains a timestamp over the signer's signature or a record must be maintained and cannot be undetectable modified, of the electronic signature and the time when the signature was first validated.

4.3 Forms of Validation Data

An electronic signature may exist in many forms including:

- the Electronic Signature (ES), which includes the digital signature and other basic information provided by the signer;
- the ES with Timestamp (ES-T), which adds a timestamp to the Electronic Signature, to take initial steps towards providing long term validity;
- the ES with Complete validation data (ES-C), which adds to the ES-T references to the complete set of data supporting the validity of the electronic signature (i.e. revocation status information).

The signer shall provide at least the ES form, but in some cases may decide to provide the ES-T form and in the extreme case could provide the ES-C form. If the signer does not provide ES-T, the verifier shall either create the ES-T on first receipt of an electronic signature or shall keep a secure record of the current time with the ES. Either of these two approaches provide independent evidence of the existence of the signature at the time it was first verified which should be near the time it was created, and so protects against later repudiation of the existence of the signature. If the signer does not provide ES-C the verifier shall create the ES-C when the complete set of revocation and other validation data is available.

The ES satisfies the legal requirements for electronic signatures as defined in the European Directive on electronic signatures, see annex C for further discussion on relationship of the present document to the Directive. It provides basic authentication and integrity protection and can be created without accessing on-line (timestamping) services. However, without the addition of a timestamp or a secure time record the electronic signature does not protect against the threat that the signer later denies having created the electronic signature (i.e. does not provide non-repudiation of its existence).

The ES-T time-stamp or time record should be created close to the time that ES was created to provide maximum protection against repudiation. At this time all the data needed to complete the validation may not be available but what information is readily available may be used to carry out some of the initial checks. For example, only part of the revocation information may be available for verification at that point in time.

Generally, the ES-C form cannot be created at the same time as the ES, as it is necessary to allow time for any revocation information to be captured. Also, if a certificate is found to be temporarily suspended, it will be necessary to wait until the end of the suspension period.

The signer should only create the ES-C in situations where it was prepared to wait for a sufficient length of time after creating the ES form before dispatching the ES-C. This, however, has the advantage that the verifier can be presented with the complete set of data supporting the validity of the ES.

Support for ES-C by the verifier is mandated (see clause 14 for specific conformance requirements).

An Electronic Signature (ES), with the additional validation data forming the ES-T and ES-C is illustrated in figure 1.