SLOVENSKI STANDARD
SIST-TS ETSI/TS 101 733 V1.5.1:2005

01-maj-2005

Elektronski podpisi in infrastruktura (ESI) – Formati elektronskega podpisa

Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats

Ta slovenski standard je istoveten z: **TS 101 733 Version 1.5.1**

ICS:

35.040	Nabori znakov in kodiranje informacij	Character sets and information coding

SIST-TS ETSI/TS 101 733 V1.5.1:2005 **en**

ETSI TS 101 733 V1.5.1 (2003-12)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats

Reference
RTS/ESI-000017

Keywords
electronic signature, security, e-commerce

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, send your comment to:
editor@etsi.org

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). 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 present document covers Electronic Signature Formats only, previous versions of this document covered both Electronic Signature Formats and Electronic Signature Policies. The aspects of Electronic Signature Policies covered by previous versions of TS 101 733 are now defined in TR 102 272.

The present document defines a number of Electronic Signature Formats, including electronic signature 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 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 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 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. It 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. This includes:

- RFC 3369 [6] "Cryptographic Message Syntax (CMS)";
- ISO/IEC 9594-8/ITU-T Recommendation X.509 [1]: "Information technology - Open Systems Interconnection - The Directory: Authentication framework";
- RFC 3280 [4] "Internet X.509 Public Key Infrastructure (PKIX) Certificate and CRL Profile";
- RFC 3261 [13] "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

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

The present document describes:

- format of Electronic Signature tokens;

In addition, the present document identifies other documents that define formats 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.

Informative annexes include:

- illustrations of extended forms of extended Electronic Signatures formats that protect against various vulnerabilities and examples of validation processes;
- descriptions and explanations of some of the concepts used in the present document. giving a rational for normative parts of the present document;
- information on protocols to interoperate with Trusted Service Providers;
- information on security considerations;
- an example structured content and MIME;
- 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.

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

[1] ITU-T Recommendation X.509 (2000)/ISO/IEC 9594-8 (2001): "Information technology - Open Systems Interconnection - The Directory: Authentication framework".

[2] Void.

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

[4] IETF RFC 3280 (1999): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

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

[6] IETF RFC 3369 (2002): "Cryptographic Message Syntax".

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

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

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

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

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

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

[13] IETF RFC 3261 (1998): " Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

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

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

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

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

[18] CWA 14171 CEN. Workshop Agreements: "Procedures for Electronic Signature Verification".

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

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

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

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

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

[24] IETF RFC 3281: "An Internet Attribute Certificate Profile for Authorization".

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

[26] IEFT RFC 2078: "Generic Security Service Application Program Interface, Version 2".

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): 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 [8].

electronic signature: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication

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

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

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

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

initial verification: a 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 which issued it

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

Rivest-Shamir-Adleman (RSA): asymmetric cryptography algorithm based on the difficulty to factorize 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 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

Subsequent Verification: a process performed by a verifier to assess the signature validity

NOTE: It 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 which 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 the signature is valid.

valid electronic signature: electronic signature which passes validation. For an EPES compliance to a signature validation policy is also required

verifier: entity that verifies evidence

NOTE 1: See ISO/IEC 13888-1 [9].

NOTE 2: 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
AARL	Attribute Authority Revocation List
ACRL	Attribute Certificate Revocation List
API	Application Program Interface
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
BES	Basic Electronic Signature
CA	Certification Authority
CAD	Card Accepting Device
CARL	Certification Authority Revocation List
CES	Classes of Electronic Signature
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CWA	CEN Workshop Agreement
DER	Distinguished Encoding Rules (for ASN.1)
DSA	Digital Signature Algorithm (see annex E on cryptographic algorithms)
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EPES	Explicit Policy-based Electronic Signature
ES	Electronic Signature
ES-A	Electronic Signature with Archive validation data
ES-C	Electronic Signature with Complete validation data
ESS	Enhanced Security Services (enhances CMS)
ES-T	Electronic Signature with Time-stamp
ES-X	Electronic Signature with eXtended validation data
IDL	Interface Definition Language
MIME	Multipurpose Internet Mail Extensions
OCSP	Online Certificate Status Provider
OID	Object IDentifier
PCK	Public Key Certificate
PKIX	internet X.509 Public Key Infrastructure
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm 1 (see annex E on cryptographic algorithms)
TSA	Time-Stamping Authority
TSP	Trusted Service Provider
TST	Time-Stamp Token
TSU	Time-Stamping Unit
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XML	eXtended Mark up Language

4 Overview

The present document defines a number of **Electronic Signature** (ES) formats that build on CMS (RFC 3369 [6] by adding signed and unsigned attributes.

This clause provides an introduction to the major parties involved (clause 4.1), the concept of Signature Policies (clause 4.2), provides an overview of the various ES formats (clause 4.3), introduces the concept of validation **data** and provides an overview of formats that incorporate validation data (clause 4.4), presents relevant considerations on arbitration (clause 4.5) and for the validation process (clause 4.6).

The formal specifications of the attributes are specified in clauses 5 and 6, annexes C and D provide rationale for the definitions of the different ES forms.

4.1 Major parties

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

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

The **signer** is the entity that 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, time-stamp 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);
- Time-Stamping Authorities;
- Time-Marking Authorities;
- Signature Policy Issuers.

Certification Authorities provide users with public key certificates and with a revocation service.

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.

Time-Stamping Authorities attest that some data was formed before a given trusted time.

Time-Marking Authorities record that some data was formed before a given trusted time.

Signature Policy Issuers define the signature policies to be used by signers and verifiers.

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 Signatures policies

The present document includes the concept of signature policies that can be used to establish technical consistency when validating electronic signatures. When a comprehensive signature policy used by the verifier is either explicitly indicated by the signer or implied by the data being signed, then a consistent result can be obtained when validating an electronic signature. When the signature policy being used by the verifier is neither indicated by the signer nor can be derived from other data, or the signature policy is incomplete then verifiers, including arbitrators, may obtain different results when validating an electronic signature. Therefore, comprehensive signature policies that ensure consistency of signature validation are recommended from both the signers and verifiers point of view.