SLOVENSKI STANDARD
SIST-TP ETSI/SR 002 176 V1.1.1:2005

01-maj-2005

Elektronski podpisi in infrastruktura (ESI) – Algoritmi in parametri za varne elektronske podpise

Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

Ta slovenski standard je istoveten z: **SR 002 176 Version 1.1.1**

ICS:

35.040	Nabori znakov in kodiranje informacij	Character sets and information coding

SIST-TP ETSI/SR 002 176 V1.1.1:2005 **en**

ETSI SR 002 176 V1.1.1 (2003-03)

Special Report

Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

Reference
DSR/ESI-000016

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, 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).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

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

Introduction

The present document provides for security and interoperability for the application of the underlying mathematical algorithms and related parameters for secure electronic signatures in accordance with the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [1].

The present document will be handed to the EC via the EESSI-SG through ICTSB as a substantial contribution to be discussed further at the A9C (Article 9 Committee) level. The final decision on how to respect and how to handle this contribution and its future handling process will be the responsibility of the EC and A9C.

The present document defines a list of approved cryptographic algorithms together with the requirements on their parameters, as well as the approved combinations of algorithms in the form of "signature suites". The approved algorithms and parameters shall be referenced in the corresponding Protection Profiles (e.g. for SSCDs or trusted CSP components).

The present document contains several informative annexes which provide useful information on a number of subjects mentioned in the text.

1 Scope

The present document defines an initial set of algorithms and the corresponding parameters to be included in a list of approved methods for producing or verifying Electronic Signatures in Secure Signature-Creating Devices (SSCD) (EESSI-work area F: CWA 14168 / 14169 Secure Signature-Creation Devices), to be referenced in the Certificate Policy documents (EESSI-work area A: TS 101 456: Policy requirements for certification authorities issuing qualified certificates), during the signature creation and validation process and environment (EESSI-work area G1/2: CWA 14170: Security Requirements for Signature Creation Systems; CWA 14171 Procedures for Electronic Signature Verification), in trusted CSP components (Certification Service Provider) (EESSI-work-area D: CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures) and other technical components and related areas.

The present document defines a list of approved cryptographic algorithms combined with the requirements on their parameters, as well as the approved combinations of algorithms in the form of "signature suites". The approved algorithms and parameters shall be referenced in the corresponding Protection Profiles (e.g. for SSCDs or trusted CSP components). To support the management activities, a numbering scheme for cryptographic algorithms and their parameters is defined.

Specifically, the present document gives guidance on

- management practices for cryptographic algorithms (see clause 4.1),
- signature suites (see clause 4.2),
- cryptographic hash functions (see clause 4.3),
- padding methods (see clause 4.4),
- signature algorithms and the corresponding key generation algorithms (see clause 4.5), and
- random-number generation (see clause 4.6).

The present document also gives guidance on the management practices that shall be applied to cope with developments such as the examples given in the annex A. It describes a process for updating the approved algorithms lists and parameters. Annex B contains OIDs assigned to the approved algorithms, annex C gives more information on the generation of RSA keys for signatures and annex D addresses the generation of random data.

Currently no algorithms are specified for symmetric encryption of critical data outside a secure device or for proving correspondence between the Signature Creation Data (SCD) and Signature Verification Data (SVD). Nonetheless such algorithms are within the scope of a subsequent version of the present document.

Patent related issues are out of the scope of the present document.

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

[2] ISO/IEC 9979 (1999): "Information technology - Security techniques - Procedures for the registration of cryptographic algorithms".

[3] IETF RFC 2459 (1999): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", Housley,R., et al.

[4] ISO/IEC 10118-3 (1998): "Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions".

[5] FIPS Publication 180-1 (1995): "Secure Hash Standard (SHS)".

[6] PKCS #1 v2.0 (1998): "RSA Cryptography Standard".

[7] ISO/IEC 14888-3 (1999): "Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms".

[8] FIPS Publication 140-1 (1994): "Security requirements for cryptographic modules".

[9] FIPS Publication 186-2 (2000): "Digital Signature Standard (DSS)".

[10] IEEE P1363 (2000): "Standard Specifications for Public-Key Cryptography".

[11] ANSI X9.62-1998 (1998): "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)".

[12] ISO/IEC 9796-3 (2000): "Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms".

[13] ISO/IEC FCD 15946-2 (1999): "Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures".

[14] ISO/IEC CD 15946-4 (2001): "Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 4: Digital signatures giving message recovery".

[15] IETF RFC 1750 (1994): "Randomness Recommendations for Security", Eastlake, D., et al.

[16] ANSIX9.17-1985 (1985): "Financial Institution Key Management (wholesale)".

[17] PKCS #1 v2.1 draft 2 (2001): "RSA Cryptography Standard".

[18] Change Recommendation for ANSI X9.30-1995, (Part 1), Draft, April 2001.

[19] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", Adams, C., et al.

3 Definitions and abbreviations

3.1 Definitions

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

bit length: The bit length of an integer p is r if $2^{r-1} \leq p < 2^r$.

Management Activity (MA): action that shall be taken by the electronic signature committee under the circumstances specified in clause 4 of SR 002 176

signature suite: combination of a signature algorithm with its parameters, a key generation algorithm, a padding method, and a cryptographic hash function

NOTE: The currently approved signature suites are specified in the present document.

3.2 Abbreviations

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

A9C	Article 9 Committee
CRL	Certification-Service-Provider
CRT	Chinese Remainder Theorem
CSP	Certification-Service-Provider
CWA	CEN Workshop Agreement
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ECGDSA	Elliptic Curve German Digital Signature Algorithm
MA	Management Activity
OID	Object Identifier
PRNG	Pseudo Random Number Generator
RSA	Rivest, Shamir and Adleman Algorithm
SCD	Signature-Creation Data
SSCD	Secure-Signature-Creation Device
SVD	Signature-Verification Data
TRNG	True Random Number Generator

4 Algorithms and Parameters for Secure Electronic Signatures

4.1 Management activities

As a response to relevant developments in the area of cryptography and technology, activities for the management of the algorithms and parameters for secure electronic signatures shall enable dynamic updating of the lists of approved algorithms and parameters. The initial lists of approved algorithms and their parameters are given in the present document.

The management activities to introduce new algorithms and their parameters and to delete algorithms and their parameters from the list need to respond to the following situations:

1) The need to introduce new algorithms and relevant parameters will call for a mechanism that is rather dynamic. Normal update cycles of the present document are not deemed to be fast enough to reflect the market need.

2) Advances in cryptography will call for a phasing out of some algorithms or parameters. Such phasing out will be known well in advance.

3) In the case of new attacks the immediate need to remove an algorithm can arise.

Through A9C, mechanisms shall be put in place that can react within 6 months for cases 1 and 2 and at most 1 month for case 3.

Further information on updating algorithms and parameters is contained in annex A.

4.2 Signature suites for secure electronic signatures

Due to possible interactions which may influence security of electronic signatures, algorithms and parameters for secure electronic signatures shall be used only in predefined combinations referred to as the signature suites. A signature suite consists of the following components:

- a signature algorithm with parameters,
- a key generation algorithm,
- a padding method, and

- a cryptographic hash function.

If any of the components of a suite has been cancelled, the suite must be cancelled as well. If any of the components of a suite has been updated, the suite must be updated as well.

The list of currently approved signature suites is given in Table 1.

Each entry in the list of signature suites shall contain a date. This date represents the last day on which the algorithm suite is to be used for producing signatures. The dates will require revision well before they are due for the mentioned suite and should be reviewed at regular intervals, e.g. annually.

For all components only short names are used. Each component is defined in a separate table in the following clauses. Object Identifiers (OIDs) are specified in annex B.

Table 1: The list of approved signature suites

Signature suite entry index	Signature algorithm	Signature algorithm parameters	Key generation algorithm	Padding method	Cryptographic hash function	Valid until (signing)
001	rsa	MinModLen=1020	rsagen1	emsa-pkcs1-v1_5	sha1	31.12.2005
002	rsa	MinModLen=1020	rsagen1	emsa-pss	sha1	31.12.2005
003	rsa	MinModLen=1020	rsagen1	emsa-pkcs1-v1_5	ripemd160	31.12.2005
004	rsa	MinModLen=1020	rsagen1	emsa-pss	ripemd160	31.12.2005
005	dsa	pMinLen=1024 qMinLen=160	dsagen1	-	sha1	31.12.2005
006	ecdsa-Fp	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	-	sha1	31.12.2005
007	ecdsa-F2m	qMinLen=160 r0Min=10^4 MinClass=200	ecgen2	-	sha1	31.12.2005
008	ecgdsa-Fp	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	-	sha1	31.12.2005
009	ecgdsa-Fp	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	-	ripemd160	31.12.2005
010	ecgdsa-F2m	qMinLen=160 r0Min=10^4 MinClass=200	ecgen2	-	sha1	31.12.2005
011	ecgdsa-F2m	qMinLen=160 r0Min=10^4 MinClass=200	ecgen2	-	ripemd160	31.12.2005

4.3 Cryptographic hash functions

A cryptographic hash function is a preimage resistant and 2nd preimage resistant function with a constant-length output used to compute the hashcode of a document to be signed. For secure electronic signatures a hash function must be collision-resistant, which means that it is computationally infeasible to find two different documents yielding the same hashcode (which implies that it is also infeasible to find a different document yielding the same hashcode as a given document).

If due to advances in cryptography or computing technology any of these conditions is no longer met, the hash function is considered insecure and must be removed from the list of approved hash functions (see clause 4.1).

The list of currently approved hash functions is given in Table 2. Each hash function has a unique entry index represented by a string beginning with "2." followed by a two-digit entry number. The relevant OIDs are given in annex B.

Table 2: The list of approved cryptographic hash functions

Hash function entry index	Short hash function entry name	Adoption date	Normative references
2.01	sha1	01.01.2001	[4] and [5]
2.02	ripemd160	01.01.2001	[4]

4.4 Padding methods

Some signature algorithms require a hashcode to be padded to up to a certain block length used with a specific algorithm setting (e.g. RSA modulus length). The present document does not specify mandatory padding methods, but requires a padding method, if required by an algorithm (as indicated in clause 4.5), to meet certain requirements defined in the given normative references.

The list of currently approved padding methods is given in Table 3. Each padding method has a unique entry index represented by a string beginning with "3." followed by a two-digit entry number.

Table 3: The list of approved padding methods

Padding method entry index	Short padding function entry name	Random number generation method	Random generator parameters	Adoption date	Normative references
3.01	emsa-pkcs1-v1_5	-	-	01.01.2001	[6], clause 9.2.1
3.02	emsa-pss	TBD	TBD	TBD	[17], clause 9.2.2

It is intended that further padding schemes will be added as and when they have been fully standardized. These include several methods based on ISO/IEC 9796-2, currently under review. The emsa-pss method is included as, despite not being finalized, it has been stable for a long time and is a good improvement to the emsa-pkcs1-v1_5 scheme.

4.5 Signature algorithms

4.5.1 General comments

A signature algorithm is applied to the hashcode of the document to be signed to generate a signature with the SCD. The algorithm to be applied for verification with the SVD must be given. Before a signature algorithm is applicable a complete set of approved parameters must be defined. It must be practically impossible to compute the SCD from the SVD.

The list of currently approved signature algorithms is given in Table 4. Each signature algorithm has a unique entry index represented by a string beginning with "1." followed by a two-digit entry number.

Note that the minimum modulus length for RSA is given as 1 020 bits rather than the more natural 1 024 bits. This is to allow for implementations that cannot use the topmost bit(s).