ETSI TS 119 312 V1.2.2 (2018-09)

Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

Reference

RTS/ESI-0019312v122

Keywords

e-commerce, electronic signature, security, trust services

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Selection of the cryptographic suites to apply for digital signatures is an important business parameter for products and services implementing digital signatures. The present document provides guidance on selection of cryptographic suites with particular emphasis on interoperability. The present document is based on the specified agreed cryptographic mechanisms of the SOG-IS Crypto Evaluation Scheme [15]. The SOG-IS Crypto WG is in charge of providing requirements and evaluation procedures related to cryptographic aspects of Common Criteria security evaluations of IT products. To avoid conflicts between the evaluation of security product for qualified trust services and the recommendation given in the present document, the ETSI Technical Committee Electronic Signatures and Infrastructures (ESI) decided to refer for the trust services [i.12], article 3 (16a) consisting of creation, verification, and validation of electronic signatures, electronic seals and electronic time stamps, electronic registered delivery services and certificates related to those services to the SOG-IS Crypto Evaluation Scheme [15].

Other standardization bodies, security agencies and supervisory authorities of the Member States have published guidance documents with partially overlapping scope, for instance (but not limited to) France [i.2] and Germany [i.3], [i.14]. These documents can be consulted as informative supplementary material when planning the implementation of trust services.

1 Scope

The present document lists cryptographic suites used for the creation and validation of digital signatures and electronic time stamps and related certificates. The present document builds on the agreed cryptographic mechanisms from SOG-IS [15]. It may be used also for electronic registered delivery services in the future.

The present document focuses on interoperability issues and does not duplicate security considerations given by other standardization bodies, security agencies or supervisory authorities of the Member States. It instead provides guidance on the selection of concrete cryptographic suites that use agreed mechanisms. The use of SOG-IS agreed mechanisms is meant to help ensure a high level of security in the recommended cryptographic suites, while the focus on specific suites of mechanisms is meant to increase interoperability and simplify design choices.

There is no normative requirement on selection among the alternatives for cryptographic suites given here but for all of them normative requirements apply to ensure security and interoperability.

The present document also provides guidance on hash functions, (digital) signature schemes and (digital) signature suites to be used with the data structures used in the context of digital signatures and seals. For each data structure, the set of algorithms to be used is specified.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

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

The following referenced documents are necessary for the application of the present document.

[1] FIPS Publication 180-4 (August 2015): "Secure Hash Standard (SHS)", National Institute of Standards and Technology.

[2] FIPS Publication 186-4 (July 2013): "Digital Signature Standard (DSS)", National Institute of Standards and Technology.

[3] IETF RFC 3447 (2003): "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1".

[4] ISO/IEC 14888-3 (2016): "Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms".

[5] IETF RFC 5639 (2010): "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation".

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

[7] IETF RFC 3279 (2002): "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

NOTE: Updated by IETF RFC 4055, IETF RFC 4491, IETF RFC 5480 and IETF RFC 5758.

[8] IETF RFC 4055 (2005): "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile".

[9] IETF RFC 5753 (2010): "Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)".

[10] IETF RFC 6931 (2013): "Additional XML Security Uniform Resource Identifiers (URIs)".

[11] W3C Recommendation: "XML Encryption Syntax and Processing Version 1.1", April 2013.

NOTE: Available at https://www.w3.org/TR/2013/REC-xmlenc-core1-20130411.

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

NOTE: Updated by IETF RFC 5816.

[13] IETF RFC 6960 (2013): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

NOTE: Updates RFC 2560, RFC 6277.

[14] W3C Recommendation: "XML Signature Syntax and Processing Version 1.1", April 2013.

NOTE: Available at https://www.w3.org/TR/2013/REC-xmldsig-core1-20130411.

[15] SOG-IS Crypto Working Group: "SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms" Version 1.0, May 2016.

NOTE: Available at https://www.sogis.org/uk/supporting_doc_en.html.

[16] FIPS Publication 202 (August 2015): "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", National Institute of Standards and Technology.

NOTE: Available at https://dx.doi.org/10.6028/NIST.FIPS.202.

[17] IETF RFC 5480 (2009): "Elliptic Curve Cryptography Subject Public Key Information".

[18] NIST: "Computer Security Objects Register (CSOR)".

NOTE: Available at https://csrc.nist.gov/groups/ST/crypto_apps_infra/csor/algorithms.html.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ENISA: "Algorithms, Key Sizes and Parameters Report, 2013 recommendations, version 1.0" (2013-10).

NOTE: Available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report.

[i.2] Agence nationale de la sécurité des systèmes d'information: "Référentiel Général de Sécurité version 2.0" (2014-06).

NOTE: Annex B1 (version 2.03 of 2014-02) is available at https://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf.

[i.3] "Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Übersicht über geeignete Algorithmen" (2015-12).

NOTE: Available at https://www.bundesnetzagentur.de.

[i.4] Void.

[i.5] ISO/IEC 10118-3 (2004): "Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions".

NOTE: This ISO Standard duplicates the standardization from FIPS Publication 180-4 [1].

[i.6] ETSI TS 101 733 (V2.2.1) (04-2013): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.7] ETSI TS 101 903 (V1.4.2) (12-2010): "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.8] ETSI TS 102 778 (parts 1 to 6): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles".

[i.9] IETF RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.10] W3C Recommendation: "Canonical XML Version 1.0" (omits comments).

NOTE: Available at https://www.w3.org/TR/2001/REC-xml-c14n-20010315.

[i.11] W3C Recommendation: "Canonical XML Version 1.0" (with Comments).

NOTE: Available at https://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718.

[i.12] Regulation (EU) No 910/2014 of the European Parliament and of the Council, July 2014.

[i.13] OID Repository http://oid-info.com.

NOTE: This OID repository is a kind of wiki where any user can add any information about any OID. It is not an official registration authority for OIDs and should be handle with care. Nevertheless it provides usually the link to corresponding official registration authority.

[i.14] Bundesamt für Sicherheit in der Informationstechnik, BSI TR-02102: "Cryptographic Mechanisms, version" (2017-01).

NOTE: Available at https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/tr02102_node.html.

[i.15] ETSI EN 319 422 (V1.1.1) (03-2016): "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[i.16] ANSSI: "Publication d'un paramétrage de courbe elliptique visant des applications de passeport électronique et de l'administration électronique française", October 2011.

NOTE: Available at https://www.ssi.gouv.fr.

[i.17] ETSI EN 319 122 (part 1 and 2): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures".

[i.18] ETSI EN 319 132 (part 1 and 2): "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures".

[i.19] ETSI EN 319 142 (part 1 and 2): "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures".

3 Definitions and abbreviations

3.1 Definitions

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

cryptographic suite: combination of a signature scheme with a padding method and a cryptographic hash function

(digital) signature: data associated to, including a cryptographic transformation of, a data unit that:

a) allows to prove the source and integrity of the data unit;

b) allows to protect the data unit against forgery; and

c) allows to support signer non-repudiation of signing the data unit.

Hash function: As defined in ISO/IEC 10118-3 [i.5].

legacy mechanism: mechanism deployed on a large scale, currently offering a security level for an acceptable short-term security but no longer representing the cryptographic state of the art [15]

NOTE: As a consequence, a validity period is defined for legacy mechanisms.

Recommended mechanism: mechanism, that fully reflects the state of the art in cryptography, providing an adequate level of security against all presently known or conjectured threats even taking into account the generally expected increases in computing power [15]

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

signature scheme: triplet of three algorithms composed of a signature creation algorithm, a signature verification algorithm and a key generation algorithm

3.2 Abbreviations

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

ANSI	American National Standards Institute
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (National Agency for Security of Information Systems)
CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CSOR	Cryptographic Algorithm Object Registration
DER	Distinguished Encoding Rules (Syntax rules for ASN.1)
DSA	Digital Signature Algorithm
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EC-DSA	Elliptic Curve Digital Signature Algorithm
ENISA	European Union Agency for Network and Information Security
ESI	Electronic Signatures and Infrastructure (Technical Committee of ETSI)
FIPS	Federal Information Processing Standard
FR	Identifier for Elliptic Curves defined by ANSSI
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
IT	Information Technology
MGF	Mask Generation Function
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol

OID	Object Identifier
PKCS	Public-Key Cryptography Standards
PSS	Probabilistic Signature Scheme
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman algorithm
SHA	Secure Hash Algorithm
SOG-IS	Senior Officials Group Information Systems Security
TST	Time-Stamp Token
TSU	Time-Stamping Unit
URI	Uniform Resource Identifier
URN	Uniform Resource Number
WG	Working Group
XML	eXtensible Markup Language

4 Use of SOG-IS Agreed Mechanisms and Maintenance of the present document

In order to avoid duplicated effort, the assessment of the security of underlying cryptographic schemes is delegated to the SOG-IS document [15].

The SOG-IS Evaluation Scheme distinguishes between **legacy mechanisms** (schemes and parameter selections which may enjoy wide deployment, but do not represent the current state of the art in cryptography) and **recommended mechanisms** (schemes and parameters which do represent the current state of the art in cryptography). The present document uses the notion of "recommended" and "legacy" primitives in the same way as [15].

In general, only SOG-IS recommended mechanisms and key sizes or cryptographic suites using these cryptographic mechanisms and key sizes should be used to generate new signatures and seals (including certificate signatures). SOG-IS legacy mechanisms may, however, still be used for this purpose when this is necessary to ensure interoperability with existing infrastructures as long as they remain agreed. For the reader's convenience, the classification of mechanisms as legacy or recommended is repeated in the present document.

The maintenance activities will follow the maintenance procedure of the SOG-IS Crypto Evaluation Scheme [15] with revisions on a two-year base. This coincides with the established schedule in ETSI ESI.

In the case of new attacks, the immediate need to remove an algorithm could arise, and a new revision of the present document will be published as soon as possible.

5 Hash functions

5.1 General

The list of hash functions in table 1 shall be used. The functions shall be implemented as per the reference listed in table 1 and shall follow the recommendations provided in the SOG-IS Agreed Cryptographic Mechanisms [15]. The present document provides additional recommendations in the following clauses.

Table 1: Agreed Hash Functions [15], p. 13

Short hash function name	References
SHA-224	FIPS Publication 180-4 [1]
SHA-256	FIPS Publication 180-4 [1]
SHA-384	FIPS Publication 180-4 [1]
SHA-512	FIPS Publication 180-4 [1]
SHA-512/256	FIPS Publication 180-4 [1]
SHA3-256	FIPS Publication 202 [16]
SHA3-384	FIPS Publication 202 [16]
SHA3-512	FIPS Publication 202 [16]