ETSI TS 119 312 V1.5.1 (2024-12)

Electronic Signatures and Trust Infrastructures (ESI);
Cryptographic Suites

Reference
RTS/ESI-0019312v1.5.1

Keywords
digital 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

List of tables

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust 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 [14]. 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 Trust 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 [14].

Other standardization bodies, security agencies and supervisory authorities of the Member States have published guidance documents with partially overlapping scope, not referenced in the present document.

1 Scope

The present document lists cryptographic suites used for the creation and validation of digital signatures and electronic timestamps and related certificates. The present document builds on the agreed cryptographic mechanisms from SOG-IS [14]. It may be used also for electronic registered delivery services in the future. In contrast to previous versions of the present document, specific end dates are provided. The present document works on the assumption that the validity period (i.e. between `notBefore` and `notAfter`) of (qualified) end-entity certificates issued by trust services providers is typically three years.

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 in the ETSI docbox.

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] NIST FIPS Publication 180-4 (August 2015): "Secure Hash Standard (SHS)".

[2] NIST FIPS Publication 186-5 (2023-02): "Digital Signature Standard (DSS)".

[3] IETF RFC 8017 (2016): "PKCS #1: RSA Cryptography Specifications Version 2.2".

[4] ISO/IEC 14888-3:2018: "IT 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] Void.

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

[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 11 April 2013: "XML Encryption Syntax and Processing Version 1.1".

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

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

[14] SOG-IS Crypto Working Group: "SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms", Version 1.3, February 2023.

[15] NIST FIPS Publication 202 (August 2015): "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions".

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

[17] Void.

[18] IETF RFC 3526: "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)".

[19] IETF RFC 5758: "Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA".

[20] IETF RFC 9231: "Additional XML Security Uniform Resource Identifiers (URIs)".

[21] IETF RFC 9688: "Use of the SHA3 One-Way Hash Functions in the Cryptographic Message Syntax (CMS)".

[22] NIST SP 800-186: "Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters".

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] European Network of Excellence in Cryptology: "Algorithms, Key Size and Protocols Report (2018)", ECRYPT - Coordination & Support, Action D5.4.

[i.2] Void.

[i.3] Void.

[i.4] Void.

[i.5] ISO/IEC 10118-3:2018: "Information technology — Security techniques — Hash functions — Part 3: Dedicated hash functions".

NOTE: This ISO Standard duplicates the standardization from FIPS Publication 180-5 [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 (2 May 2008): "Canonical XML Version 1.1".

[i.11] W3C® Recommendation (18 July 2002): "Exclusive XML Canonicalization Version 1.0".

[i.12] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.13] OID Repository.

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] Void.

[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] Void.

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

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

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

[i.20] ETSI EN 319 102-1: "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.21] ANSSI: "Avis relatif aux paramètres de courbes elliptiques définis pas l'État français". In: Journal Officiel 0241 (October 2011), p. 17533.

[i.22] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[i.23] Fukang Liu et al.: "Analysis of RIPEMD-160: New Collision Attacks and Finding Characteristics with MILP".

[i.24] Marc Stevens et al.: "The first collision for full SHA-1".

[i.25] Thorsten Kleinjung et al.: "Factorization of a 768-bit RSA modulus".

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

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

AdES (digital) signature: digital signature that is either a CAdES signature, or a PAdES signature or a XAdES signature

CAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 122 (parts 1 and 2) [i.17]

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 of at least 100 bits and considered to provide an acceptable short-term security but which should be phased out as soon as practical because no longer fully reflecting the state of the art and suffering from some security assurance limitations

PAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 142 (parts 1 and 2) [i.19]

recommended mechanism: mechanism, that fully reflects the state of the art in cryptography, currently offers a security level of at least 125 bits, supported by strong security arguments and can be said to provide an adequate level of security against all presently known or conjectured threats even considering the generally expected increases in computing power

security level: number of operations necessary for an adversary to successfully break the security provided by the mechanism, expressed as a base 2 logarithm

NOTE 1: Security level is expressed as a base 2 logarithm, e.g. 100 bits of security means that 2^{100} operations are necessary.

NOTE 2: As defined in [14].

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

XAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 132 (parts 1 and 2) [i.18]

3.2 Symbols

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

FR	Identifier for Elliptic Curves defined by ANSSI

3.3 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
DLOG	Discrete Logarithm
DSA	Digital Signature Algorithm

EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EC-DSA	Elliptic Curve Digital Signature Algorithm
EC-SDSA-opt	optimized Elliptic Curve Schnorr Digital Signature Algorithm
ESI	Electronic Signatures and Trust Infrastructure

NOTE: A Technical Committee of ETSI.

FF	Finite Field
FIPS	Federal Information Processing Standard
GDSA	German Digital Signature Algorithm
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
PDF	Portable Document Format
PKCS	Public-Key Cryptography Standards
PSS	Probabilistic Signature Scheme
RFC	Request For Comments
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman algorithm
SDSA	Schnorr Digital Signature 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

3.4 Notations

The requirements identified in the present document include the following notations for the classification of mechanisms as legacy mechanisms or recommended mechanisms:

L: denotes a legacy mechanism with a deprecation/phasing out date of 31.12.2033 and which might be extended with future releases of the present document.

NOTE: In contrast to [14] and to reflect the assumed typical validity period of end-entity certificates issued by trust service providers as laid out in the Scope, a default of three years is added to all the end dates in the present document.

L[yyyy]: denotes a legacy mechanism with a deprecation/phasing out date no later than 31.12.yyyy, where yyyy is an integer expressing a year.

L[yyyy+]: denotes a legacy mechanism with a deprecation/phasing out date of 31.12.yyyy, where yyyy is an integer expressing a year and which might be extended with future releases of this document.

NOTE: L is semantically equivalent to L[2033+].

R: denotes a recommended mechanism which has no defined end date, yet.