ETSI TR 119 300 V1.2.1 (2016-03)

Electronic Signatures and Infrastructures (ESI);
Guidance on the use of standards for cryptographic suites

Reference
RTR/ESI-0019300v121

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

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 (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.

Foreword

This Technical Report (TR) 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.

1 Scope

The present document provides business driven guidance on the use of standards for cryptographic suites, and in particular for digital signature creation algorithms.

The present document explains the concept of security parameters that helps to choose a proper cryptographic suite for digital signature creation. It also gives an overview how to analyze the business needs and how to select a system that satisfies these needs.

The purported audience of the present document is mainly the application designers and implementers. The present document provides recommendations to trust service providers and manufacturers of security devices.

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 http://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.

Not applicable.

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] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for creation and validation of AdES digital signatures; Part 1: Creation and validation".

[i.2] ETSI TS 103 174: "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

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

NOTE: This ISO Standard duplicates FIPS Publication 180-4 [i.4].

[i.4] FIPS Publication 180-4 (2012): "Secure Hash Standard (SHS)".

[i.5] 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.6] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.7] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.8] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.9] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles".

[i.10] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[i.11] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[i.12] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[i.13] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[i.14] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.15] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.16] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.17] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.18] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.19] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.20] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[i.21] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.21] and the following apply:

NOTE: The following definitions are being imported in the present document for the sake of reader's convenience.

advanced electronic signature: As defined in Regulation (EU) No 910/2014 [i.5].

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

(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

electronic signature: As defined in Regulation (EU) No 910/2014 [i.5].

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

signature augmentation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their augmentation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

NOTE: This covers collection of information and creation of new structures that allows performing, on the long term, validations of a signature.

signature creation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their creation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

signature policy: signature creation policy, signature augmentation policy, signature validation policy or any combination thereof, applicable to the same signature or set of signatures

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

signature validation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their validation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be valid

trust service: electronic service which enhances trust and confidence in electronic transactions

trust service provider: natural or a legal person who provides one or more trust services

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 119 312 [i.6] and the following apply:

CMS	Cryptographic Message Syntax
ENISA	European Union Agency for Network and Information Security
EU	European Union
ISO	International Organization for Standardization
PDF	Portable Document Format
PIN	Personal Identification Number
TR	Technical Report
TS	Technical Specification
XML	eXtensible Markup Language

NOTE: See http://encyclopedia2.thefreedictionary.com/Extensible+Markup+Language.

4 Introduction to cryptographic suites

4.1 General

A cryptographic suite is a set of standardized algorithms which are used to create a digital signature.

The creation of a signature usually includes different digital signature creation algorithms.

Moreover the creation of certificates, used for signer identification and the integration of timing information is also based on digital signature algorithms. Therefore the selection of the cryptographic suite is not a task for a single signature creation but will appear in different business processes as well as in the systems design.

In the following the components of a cryptographic suite and how they are related to the overall security level are considered.

4.2 Digital signatures

ETSI EN 319 102-1 [i.1] specifies procedures for creating and augmenting digital signatures in a format-agnostic way. It introduces general principles, objects and functions relevant when creating and augmenting signatures. It also defines general forms of digital signatures that increase their longevity. It is based on the use of public key cryptography to produce such signatures, which are supported by public key certificates.

The policy requirements, the syntax of the signature (XML, CMS or PDF), the relationship between the signature and the data object that is signed (enveloped, enveloping or detached), the relationship between signatures (single, parallel or countersignature), the commitment, the timing information, attributes or identity of the signer are not relevant for the cryptographic algorithm for creating a digital signature. Nevertheless the security of the digital signature heavily depends on them.

4.3 Signature creation and verification

The digital signature creation consists of a data input encoding, including the formatting, and the cryptographic key (signer's private key) application algorithm. The output will be included as the digital signature of a document, a time-stamp or an archival signature over a (signed or unsigned) document.

The digital signature verification consists of the same data input encoding and a cryptographic key (signer's public key) application algorithm. The output of the verification is either "valid" or "invalid".

4.4 Cryptographic algorithms

4.4.1 Hash functions

The data to be signed can be of different nature and format. Before a signature can be applied it is binary encoded in a canonical way. Additionally, the data input encoding makes use of a hash function, that transforms (compresses) the binary input data to a short hash value for which the cryptographic signature algorithm is applicable.

Since the signature creation will be based on the hash function output it is important to have a cryptographically strong hash function, that is computationally hard to invert (this prevents blank signatures without a finalized document to be signed), collision resistant and pre-image resistant.

Collision resistance prevents the preparation of two or more documents with the same signature, whereas the pre-image resistance prevents the creation of a second document that hashes to the same value as an already signed document.

Any hash function has the output length as a parameter. The encoding of the output as a bit string gives the "bit length" parameter of the dedicated hash function.

The bit length is an upper bound for the security level of the hash function. More details are given in clause 5.

4.4.2 Message encoding and random numbers

The hash value derived from the binary encoded input data is used as input to the signature creation algorithm. A pre-formatting (message encoding) creates the digital signature input data. Additionally, a randomization is used, that results in different signatures for every application of the algorithms. The quality of the random values used for the signature creation algorithm is an important security parameter. More details are given in clause 5.

4.4.3 Asymmetric signature algorithms

A digital signature creation algorithm uses the private signature creation data associated with the signer (private or secret key). The output of the algorithm is integrated in the digital signature of the signed data object.

For the signature verification a corresponding algorithm based on the signer's public verification data (public key) is used. Its input is the same binary data as used for signature creation and the thereby created digital signature. Its output is either "valid" or "invalid".

This pair of algorithms used for signature creation and verification is commonly called the signature algorithm. The key pair associated with the signer defines a security parameter, the key length, which determines the cryptographic strength of the algorithm. The security of the algorithm depends on the state-of-the-art of cryptography, i.e. the costs of the best known attack. Due to the increasing power of computational devices and the progress in cryptanalysis, the cryptographic algorithms can weaken in time.

4.4.4 Security bits

The cryptographic strength is usually measured in bits, corresponding to an upper bound for operations needed for an attack against the signature algorithm.

Breaking the signature algorithm means, that given the public verification key and some signatures for some data, the attacker can create a signature for another document without the signature creation data.

If the attack requires 2^n operations, then the cryptographic strength is denoted by n.

4.5 Standardization

4.5.1 Standardization bodies

Standardization plays an important role in the business process for implementing generation and validation of digital signatures. The cryptographic algorithms should be public and approved by independent expert groups.

All cryptographic algorithms used in ETSI TS 119 312 [i.6] are standardized by ISO. Because many of these standards originate in former national standards or other technical specifications, some of these references are given too.

4.5.2 Technical specifications

ETSI TS 119 312 [i.6] recommends algorithms suitable for digital signature creation and the conditions for their uses. For each algorithm, it defines requirements and is based on various security recommendations given by other standardization bodies, security agencies and supervisory authorities of the EU Member States. National cryptographic recommendations are considered. Whereas all listed algorithms have been checked for security, it cannot be concluded, that an algorithm not listed would be insecure. These algorithms are already in use in many other applications and can be selected by the security parameters at different strengths.

5 Selecting an appropriate signature suite

5.1 Introduction

Use of digital signatures in a business process should be defined integral to the process specification, with resulting requirements on functionality and security of the signatures, hence leading to selection of standards, profiles and parameters.

Different formats of signatures are defined in [i.2], [i.7], [i.8], [i.9], [i.10], [i.11], [i.12], [i.13], [i.14], [i.15], [i.16], [i.17], [i.18], [i.19], [i.20]. All formats can potentially use the same cryptographic functions described in clause 4.4. To support interoperability some standards do not implement all of them. These technical details are addressed in ETSI TS 119 312 [i.6].

There is no absolute scale of security. A security algorithm can be secure for one application but insecure for another. Therefore the needs of the business process should be analyzed carefully before the requirements for the signature algorithm can be identified. Beside technical conditions like the reliability for short or long term validation, legal/regulatory requirements specific to the identified application can also apply.

Almost all security breaches for signature algorithms in the past came up slowly. To date, long before an algorithm was really broken, it was already known that the security of the algorithm was called into question. Recommendations on security evaluation of signature suites are given in ETSI TS 119 312 [i.6].

A very important condition for a signature infrastructure is interoperability. The present document not only provides a guidance how to select security parameters but recommends also to select a widely deployed and commonly used signature suite. The restriction to a small set of signature algorithms does not mean that other algorithms are not secure but provides more interoperability.

5.2 Evaluating pre-conditions

5.2.1 Trust level

The business impact from a broken algorithm is important. Therefore, ETSI TS 119 312 [i.6] recommends only algorithms, where no security vulnerabilities are known. Nevertheless the security parameters of the cryptographic keys can be selected differently.

The security parameter of a key in a hierarchical infrastructure should be selected the stronger the higher the security level of the key. If an end user key becomes weak, then a new key can be issued. But a weakened key of a trust anchor requires special maintenance procedures or even the replacement of the infrastructure itself.

Therefore the security parameters of keys, on which the end user's signature validation relies, e.g. keys of certification authorities, time stamping units, archival services, should be selected stronger than the end user's signature keys. A table of security parameters of the recommended algorithms versus the trust level is given in ETSI TS 119 312 [i.6].

5.2.2 Trust period

The security parameter of a key should remain secure during the time period during which the key will be used. This concerns not only the signature creation key but also the verification key. The end user's signature creation key will be used normally all the lifetime of the key and if the key becomes weak, a new key can be issued immediately. After the end of intended key usage the signature key should be destroyed.

The verification key of a certification authority is necessary for signature validation of end user keys and should resist for a longer time. Therefore the security parameters of keys, needed for signature key validation, as keys of certification authorities, time stamping units, or archival services should be selected according to intended validation time frame and stronger than the primary signature keys. A table of security parameters of the recommended algorithms versus the usage time is given in ETSI TS 119 312 [i.6].

5.2.3 Hardware security

The security of the hardware is not an issue for the selection of cryptographic algorithms, the algorithms recommended in ETSI TS 119 312 [i.6] are all available in specialized hardware and implementation.

Nevertheless the security requirements can raise the hardware costs. In many cases the available hardware gives an upper bound for the security parameters. Taking this into account a corresponding usage time of the signature creation device can be determined according to clause 5.2.2.

5.2.4 Attack potential

The motivation and resources of an attacker depend on the value of the target. Therefore the security parameter for a key used for signatures with little value can resist much longer than keys for signatures of very high value. As noted before, the impact of a broken end user key is restricted to this key only and can be reduced to the cost of the issuance of a new key and where applicable, a new signature creation device.

On the other side, a weak or broken key of a trust anchor requires special maintenance procedures for keys relying on that trust anchor or even the partial replacement of the implemented infrastructure.

5.3 Guidance to selection

5.3.1 National supervisory bodies

A harmonized and comparable security level of signature services provides more interoperability and supports the application of digital signatures. With Regulation (EU) No 910/2014 [i.5], information on security breaches regarding trust service providers subject to the Regulation will be provided by national supervisory bodies to the European Commission and to the European Network and Information Security Agency (ENISA).

5.3.2 Trust service providers

The trust service providers select the public key algorithm and the key length for the certificate holders, taking into account: capabilities of signature creation devices to use, software support for verification algorithm, the efficiency of the algorithm (processing) for signing and validation in relevant environments, the security requirements, and the applicable legislation.

The trust service providers guarantee the homogeneity of the infrastructure by selecting the cryptographic suites to be used by their customers.

The trust service providers select cryptographic suites for their own needs, e.g. algorithm for signing of user certificates and other certificates. This guarantees the security level of the infrastructure.

The trust service providers should select the appropriate cryptographic suite at the security level that fits their needs. Interoperability and standardization requirements may be the most important issue.

The selection of the cryptographic suite should take the conditions listed in clause 5.2 into account.

5.3.3 Manufacturers of security devices

Manufacturer of security devices should implement the secret key algorithms at the specified key sizes. There should be trust service providers being able to certify the keys, and there should be software support for the selected algorithms (interoperability).

5.3.4 Information to end users

End users creating signatures in a business process are faced with processing (efficiency) requirements, security requirements, regulatory requirements, and interoperability requirements. The trust service provider ensures that the security requirements are fulfilled. Other requirements as e.g. PIN management are more important for the end users than the cryptographic suite selection. The trust service provider informs the end users about the relevant requirements.

End users in need of signature validation can use software (possibly hardware too) or a service that support validation of all cryptographic suites they want to accept. The trust service provider gives recommendations and advices.

Based on the usage time of signature creation key and the time frame, for which the signature should remain verifiable and secure, a time parameter can be derived, which can be used to select according to ETSI TS 119 312 [i.6] a suitable set of cryptographic algorithms together with their parameters.

Annex A: Bibliography

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

NOTE: This Directive and its implementations in EU Member States legislation are the applicable European legislation until 1 July 2016 at which date the Directive will be repealed by Regulation (EU) No 910/2014 [i.5].

- ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

History

Document history		
V1.1.1	May 2015	Publication
V1.2.1	March 2016	Publication