ETSI TR 119 001 V1.2.1 (2016-03)

Electronic Signatures and Infrastructures (ESI);
The framework for standardization of signatures;
Definitions and abbreviations

Reference
RTR/ESI-0019001v121

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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 definitions and abbreviations for use in the ETSI ESI framework for standardization of signatures.

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.

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

[i.1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. OJ L 13, 19.1.2000, p. 12-20.

[i.2] 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. OJ L 257, 28.8.2014, p. 73-114.

[i.3] Recommendation ITU-T X.800 (1991): "Security Architecture for Open Systems Interconnection for CCITT applications".

[i.4] ISO 7498-2:1989: "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture".

[i.5] Recommendation ITU-T X.1252 (2010): "Cyberspace security - Identity management - Baseline identity management terms and definitions".

[i.6] Recommendation ITU-T X.509 (ISO/IEC 9594-8): "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.7] 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.5].

[i.8] ISO/IEC 17000:2004: "Conformity assessment -- Vocabulary and general principles".

[i.9] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".

[i.10] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.11] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

[i.12] BIPM Circular T.

NOTE: Available from the BIPM website http://www.bipm.org/.

[i.13] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[i.14] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[i.15] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

[i.16] W3C Recommendation: "XML-Signature Syntax and Processing. Version 1.1".

[i.17] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.18] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[i.19] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.20] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.21] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.22] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.23] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.24] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.25] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.26] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[i.27] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[i.28] ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".

[i.29] IETF RFC 2315: "PKCS #7: Cryptographic Message Syntax Version 1.5".

[i.30] IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".

[i.31] IETF RFC 6838: "Media Type Specifications and Registration Procedures".

[i.32] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[i.33] ISO 15489-1: "Information and documentation -- Records management -- Part 1: General".

[i.34] Application Note: "APPNOTE.TXT - .ZIP File Format Specification", PKWARE® Inc., September 2012.

NOTE: Available at http://www.pkware.com/documents/APPNOTE/APPNOTE-6.3.3.TXT.

[i.35] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.36] ISO/IEC 9594-8: "Information technology -- Open Systems Interconnection -- The Directory -- Part 8: Public-key and attribute certificate frameworks".

[i.37] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93. OJ L 218, 13.8.2008, p. 30-47.

[i.38] 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.39] ISO/IEC 24760-1:2011: "Information Technology - Security Techniques - A framework for identity management - Part 1: Terminology and concepts".

[i.40] GlobalPlatform Device Technology - TEE System Architecture, Version 1.0, December 2011.

[i.41] ETSI TS 102 778 (all parts): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles".

[i.42] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[i.43] ETSI TS 103 174: "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

[i.44] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.45] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.46] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers".

[i.47] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in Recommendation ITU-T X.800 [i.3], ISO 7498-2 [i.4], Recommendation ITU-T X.509 [i.6], ISO/IEC 9594-8 [i.36] and the following apply:

NOTE: These definitions apply in the ETSI ESI framework for standardization of signatures.

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

advanced electronic seal: As defined in Regulation (EU) No 910/2014 [i.2].

advanced electronic signature: As defined in Regulation (EU) No 910/2014 [i.2].

advanced electronic signature under e-signature Directive: advanced electronic signature as defined in Directive 1999/93/EC [i.1], as of 1 July 2016 repealed by Regulation (EU) No 910/2014 [i.2]

approval: assertion that a trust service, falling within the oversight of a particular scheme, has been either positively endorsed or assessed for compliance against the relevant requirements (active approval) or has received no explicit restriction since the time at which the scheme was aware of the existence of the said service (passive approval)

approval scheme: any organized process of supervision, monitoring, assessment or such practices that are intended to apply oversight with the objective of ensuring adherence to specific criteria in order to maintain trust in the services under the scope of the scheme

ASiCArchiveManifest file: container file whose name matches "*ASiCArchiveManifest*.xml" containing one ASiCManifest element instance conforming to clause A.7 of ETSI EN 319 162-1 [i.46]

ASiCEvidenceRecordManifest file: container file used in ASiC-E to reference a set of files to which an ER applies whose name matches "META-INF/ASiCEvidenceRecordManifest*.xml" and containing one ASiCManifest element instance conformant to clause A.4 of ETSI EN 319 162-1 [i.46]

ASiCManifest file: file whose name matches "*ASiCManifest*.xml" containing one ASiCManifest element instance conformant to clause A.4 of ETSI EN 319 162-1 [i.46]

associated signature container: file holding data objects with related manifest, metadata and associated digital signature(s), under a specified hierarchy

attribute authority: authority which assigns privileges by issuing attribute certificates

attribute certificate: data structure, digitally signed by an attribute authority, that binds some attribute values with identification information about its holder

auditor: person who assesses conformity to requirements as specified in a given requirements document

business scoping parameter: specific parameter scoped in the light of the business process(es) where digital signatures or trust services are to be implemented, which implementers need to take into consideration for appropriately addressing the related business requirements in their implementation

CAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 122-1 [i.19] or ETSI EN 319 122-2 [i.20]

CA-certificate: public-key certificate for one CA issued by another CA or by the same CA

certificate: See public key certificate.

certificate identifier: unambiguous identifier of a certificate

certificate path (chain) validation: process of verifying and confirming that a certificate path (chain) is valid

certificate policy: named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

NOTE: This is a specific type of trust service policy.

certificate revocation list: signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

certificate validation: process of verifying and confirming that a certificate is valid

certification authority: authority trusted by one or more users to create and assign public-key certificates

NOTE 1: Optionally the certification authority can create the subjects' keys.

NOTE 2: A certification authority can be:

1) a trust service provider that creates and assigns public key certificates; or

2) a technical certificate generation service that is used by a certification service provider that creates and assign public key certificates.

certification authority revocation list: revocation list containing a list of CA-certificates issued to certification authorities that are no longer considered valid by the certificate issuer

certification path: ordered list of one or more public-key certificates, starting with a public-key certificate signed by the trust anchor, and ending with the public key certificate to be validated

NOTE: All intermediate public-key certificates, if any, are CA-certificates in which the subject of the preceding certificate is the issuer of the following certificate.

certification practice statement: statement of the practices which a certification authority employs in issuing managing, revoking, and renewing or re-keying certificates

NOTE 1: See IETF RFC 3647 [i.10].

NOTE 2: This is a specific type of trust service practice statement.

certification service provider: As defined in Directive 1999/93/EC [i.1].

certification signature: digital signature that is used in conjunction with Modification Detection Permissions (MDP)

NOTE: As defined by ISO 32000-1 [i.28], clause 12.8.2.2.

chain model: model for validation of X.509 certificate chains where all CA certificates have to be valid at the time they were used for issuing a certificate and the end-entity certificate was valid when creating the signature

claimed signing time: time of signing claimed by the signer which on its own does not provide independent evidence of the actual signing time

(signature) commitment type: signer-selected indication of the exact implication of a digital signature

(signature) constraints: abstract formulation of rules, values, ranges and computation results that a digital signature can be validated against

NOTE: Constraints can be defined in a formal signature policy, can be given in configuration parameter files or implied by the behaviour of the SVA.

(signature) creation constraints: abstract formulation of rules, values, ranges and computation results that are used when creating a digital signature

conformity assessment: process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled

NOTE: As defined in Regulation (EC) No 765/2008 [i.37] and ISO/IEC 17000:2004 [i.8], section 2.1.

conformity assessment body: body that performs conformity assessment services which is accredited as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides

NOTE: This is equivalent to conformity assessment body as specified in point 13 Article 2 of Regulation (EC) No 765/2008 [i.37].

(signature) constraints: abstract formulation of rules, values, ranges and computation results that a digital signature can be validated against

competence: ability to apply knowledge and skills to achieve intended results

container: file created according to ZIP holding as internal elements files with related manifest, metadata and associated signature(s), under a folder hierarchy

coordinated universal time: time scale based on the second

NOTE 1: As defined in Recommendation ITU-R TF.460-6 [i.9].

NOTE 2: For most practical purposes the coordinated universal time is equivalent to mean solar time at the prime meridian (0°). More specifically, it is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and solar time derived from the irregular Earth rotation (related to the Greenwich mean sidereal time (GMST) by a conventional relationship).

cross certificate: certificate that is used to establish a trust relationship between two certification authorities

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

cryptographic system: collection of transformations, normally defined by a mathematical algorithm, from plain text into cipher text and vice versa, the particular transformation(s) to be used being selected by (private or public) keys

data object: actual binary/octet data being operated on (transformed, digested, or signed) by an application

NOTE: This definition is part of the definition of this term within XMLDSIG [i.16].

data integrity: property that data has not been altered or destroyed in an unauthorized manner

data origin authentication: corroboration that the source of data received is as claimed

data to be signed formatted: data created from the data to be signed objects by formatting them and placing them in the correct sequence for the computation of the data to be signed representation

data to be signed representation: hash of the data to be signed formatted, which is used to compute the digital signature value

detached (digital) signature: digital signature that, with respect to the signed data object, is neither enveloping nor enveloped

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

digital signature value: result of the 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

domain validation certificate: certificate which has no validated organizational identity information for the subject and only identifies the subject by its domain name

driving application: application that uses a signature creation system to create a signature or a signature validation application in order to validate digital signatures or a signature augmentation application to augment digital signatures

electronic document: any content stored in electronic form, in particular text or sound, visual or audio-visual recording

electronic signature: As defined in Regulation (EU) No 910/2014 [i.2].

enveloped (digital) signature: digital signature embedded within the signed data object

enveloping (digital) signature: digital signature embedding the signed data object

EU qualified certificate: qualified certificate as specified in Directive 1999/93/EC [i.1] or in Regulation (EU) No 910/2014 [i.2] whichever is in force at the time of issuance

EU qualified trust service provider: trust service provider that meets the requirements for qualified trust service providers laid down in Regulation (EU) 910/2014 [i.2]

EV certificate: See extended validation certificate.

evidence: information that can be used to resolve a dispute about various aspects of authenticity of archived data objects

evidence record: unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time

NOTE: See IETF RFC 4998 [i.35] and IETF RFC 6283 [i.44].

extended validation certificate: As defined in CA/Browser Forum [i.11].

generator: any party which creates, or augments a digital signature

NOTE: This can be the signer or any party that initially validates or further maintains the signature.

hash function: As defined in ISO/IEC 10118-3 [i.7].

high security zone: physical location where a CA's private key or cryptographic hardware is located

identity provider: entity that makes available identity information

NOTE: See ISO/IEC 24760-1 [i.39].

legacy ASiC 102 918 container: associated signature container generated according to ETSI TS 102 918 [i.42]

legacy ASiC baseline container: digital signature generated according to ETSI TS 103 174 [i.43]

legacy ASiC container: legacy ASiC 102 918 container or legacy ASiC baseline container

legacy CAdES 101 733 signature: digital signature generated according to ETSI TS 101 733 [i.25]

legacy CAdES baseline signature: digital signature generated according to ETSI TS 103 173 [i.26]

legacy CAdES signature: legacy CAdES 101 733 signature or a legacy CAdES baseline signature

legacy PAdES 102 778 signature: digital signature generated according to ETSI TS 102 778 [i.41]

legacy PAdES baseline signature: digital signature generated according to ETSI TS 103 172 [i.27]

legacy PAdES signature: legacy PAdES 102 778 signature or a legacy PAdES baseline signature

legacy XAdES 101 903 signature: digital signature generated according to ETSI TS 101 903 [i.17]

legacy XAdES baseline signature: digital signature generated according to ETSI TS 103 171 [i.18]

legacy XAdES signature: legacy XAdES 101 903 signature or legacy XAdES baseline signature

media type: method to label arbitrary content, carried by MIME IETF RFC 2045 [i.32] or other protocols

NOTE: Refer to IETF RFC 6838 [i.31], clause 1.

message imprint: digest value of the data that is going to be time-stamped

NOTE: In the case of time-stamp tokens, it corresponds to the digest value incorporated into the `hashedMessage` field of `MessageImprint` type.

metadata: data describing context, content and structure of data objects and their management over time

NOTE: Refer to ISO 15489-1 [i.33], definition 3.12 with modifications.

mobile device: personal device which can communicate over a mobile network, usually a device suitable for carrying in hand, purse or pocket such as a mobile or smart phone

mobile network: communications network operated specifically for mobile devices, usually requiring the mobile devices to incorporate a UICC in order to communicate

mobile network operator: entity which offers mobile network services

mobile signature service: facility that coordinates and manages the process by which an end user can sign a document, or other information, using a signing key on or connected to a personal device

NOTE: This service supports local signing only.

mobile signature service provider: provider of a mobile signature service

national accreditation body: sole body in a State that performs accreditation with authority derived from the State

NOTE: This is equivalent to national accreditation body as specified in point 11 Article 2 of Regulation (EC) No 765/2008 [i.37].

organizational validation certificate: certificate that includes validated organizational identity information for the subject

PAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 142-1 [i.23] or ETSI EN 319 142-2 [i.24]

PDF serial signature: specific digital signature where the second (and subsequent) signers of a PDF not only sign the document but also the signature of the previous signer and any modification that can also have taken place (e.g. form fill-in)

PDF signature: DER-encoded binary data object based on the PKCS #7 IETF RFC 2315 [i.29] or the CMS (IETF RFC 5652 [i.30]) or related syntax containing a digital signature and other information necessary to validate the electronic signature such as the signer's certificate along with any supplied revocation information placed within a PDF document structure

NOTE 1: As specified in ISO 32000-1 [i.28], clause 12.8.

NOTE 2: Electronic signature in this definition is to be understood as a digital signature.

personal device: networked device that is assumed to be under the sole control of a natural person at the time of signing/validation

NOTE: The term personal device includes mobile devices as well as other general computing devices such as personal computers, tablets and laptops.

private key: in a public key cryptographic system, that key of an entity's key pair which is known only by that entity

proof of existence: evidence that proves that an object existed at a specific date/time

proof of integrity: evidence that proves the accuracy and completeness of an object

prospective certificate chain: sequence of n certificates which satisfies the conditions (a) to (c) in IETF RFC 5280 [i.45], clause 6.1, and the trust anchor is trusted according to the signature validation policy in use

public key: in a public key cryptographic system, that key of an entity's key pair which is publicly known

public key certificate: public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it

public key infrastructure: infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services

publicly-trusted certificate: certificate that is trusted by virtue of the fact that its corresponding root certificate is distributed as a trust anchor in widely-available application software

QCStatement: statement for inclusion in a qcStatements certificates extension

NOTE: As specified in IETF RFC 3739 [i.14].

qualified certificate under e-signature Directive: public key certificate which meets the requirements laid down in Directive 1999/93/EC [i.1] annex I, and is provided by a certification service provider who fulfils the requirements laid down in its annex II, repealed as of 1 July 2016 by Regulation (EU) No 910/2014 [i.2]

qualified electronic seal: As defined in Regulation (EU) No 910/2014 [i.2].

qualified electronic signature: As defined in Regulation (EU) No 910/2014 [i.2].

qualified electronic signature/seal creation device: As specified in Regulation (EU) No 910/2014 [i.2].

registration authority: entity that is responsible for identification and authentication of subjects of certificates mainly

NOTE 1: See IETF RFC 3647 [i.10].

NOTE 2: A registration authority can assist in the certificate application process or revocation process or both.

registration officer: person responsible for verifying information that is necessary for certificate issuance and approval of certification requests

relying party: natural or legal person that relies upon an electronic identification or a trust service

NOTE: Relying parties include parties verifying a digital signature using a public key certificate.

repudiation: denial by one of the entities involved in a communication of having participated in all or part of the communication

revocation officer: person responsible for operating certificate status changes

root CA: certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)

NOTE 1: A root CA certificate is generally self-signed but the root CA can also be certified by a (root) CA from another domain (e.g. cross-certification, root-signed in the context of a root-signing program).

NOTE 2: A root CA can be used as the trust anchor for many applications (e.g. browsers) but nothing prevents the TSP to present subordinate CAs for this purpose, according to the business context.

seal creator: As defined in Regulation (EU) No 910/2014 [i.2].

scheme operator: body responsible for the operation and/or management of any kind of assessment scheme, whether they are governmental, industry or private, etc.

secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

secure element: tamper resistant component used in a personal device to provide security, confidentiality, and multiple application environments required to support various business models

NOTE 1: Examples of secure element technologies currently used for mobile devices are UICC (also known as SIM card), embedded secure element, smartSD, smart microSD. An external secure device, such as a smart card, can also be used with a personal device to support local signing.

NOTE 2: A secure element can be a qualified electronic signature (or seal) creation device as specified in Regulation (EU) No 910/2014 [i.2] if it meets the requirements of this regulation.

secure signature creation device: As defined in Directive 1999/93/EC [i.1].

secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

secure zone: area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the systems used by the trust service provider

seed value dictionary: PDF data structure, of type dictionary, as described in ISO 32000-1 [i.28], clause 12.7.4.5, table 234, that contains information that constrains the properties of a digital signature that is applied to a specific signature field

shell model: model for validation of X.509 certificate chains where all certificates have to be valid at a given time

NOTE: The given time is an input parameter to the validation.

signatory: As defined in in Regulation (EU) No 910/2014 [i.2].

signature attribute: signature property

signature application practice statement: set of rules applicable to the application and/or its environment implementing the creation, the augmentation and/or the validation of digital signatures

signature augmentation: process of incorporating to a digital signature information aiming to maintain the validity of that signature over the long term

NOTE: Augmenting signatures is a co-lateral process to the validation of signatures, namely the process by which certain material (e.g. time stamps, validation data and even archival-related material) is incorporated to the signatures for making them more resilient to change or for enlarging their longevity.

signature augmentation application: application that implements signature augmentation

NOTE 1: The signature augmentation application takes inputs from and provides the augmented signature to a driving application.

NOTE 2: The signature augmentation application can be implemented as part of the signature creation application or as part of the signature validation application or as a stand-alone application.

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 class: set of signatures achieving a given functionality

NOTE 1: ETSI EN 319 102-1 [i.38] describes different signature classes.

NOTE 2: A signature class is implementation independent.

EXAMPLE: Signature with time, signature with long term validation material, Signature providing Long Term Availability and Integrity of Validation Material are possible signature classes.

signature creation application: application within the signature creation system, complementing the signature creation device, that creates a signature data object

signature creation data: unique data, such as codes or private cryptographic keys, which are used by the signer to create a digital signature value

signature creation device: configured software or hardware used to implement the signature creation data and to create a digital signature value

signature creation environment: physical, geographical and computational environment of the signature creation system

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 creation system: overall system, consisting of the signature creation application and the signature creation device, that creates a digital signature

signature dictionary: PDF data structure, of type dictionary, as described in ISO 32000-1 [i.28], clause 12.8.1, table 252 that contains all information about the digital signature

signature handler: software application, or part of a software application, that knows how to perform digital signature operations (e.g. signing and/or validating) in conformance with ISO 32000-1 [i.28] and the requirements of the appropriate profile

signature invocation: non-trivial interaction between the signer and the SCA or QSCD/SSCD/SCDev that is necessary to invoke the start of the signing process in the SCA/QSCD/SSCD/SCDev to generate the signed data object

NOTE: It is the 'Wilful Act' of the signer.

signature level: format specific definition of a set of data incorporated into a digital signature, which allows to implement a signature class

EXAMPLE: CAdES-B-B, CAdES-E-EPES [i.19] and [i.20], XAdES-B-LTA, XAdES-E-C [i.21] and [i.22], PAdES-B-T, PAdES-E-LTV [i.23] and [i.24] are examples of signature levels.

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 policy authority: entity responsible for the drafting, registering, maintaining, issuing and updating of a signature policy

signature policy document: document expressing one or more signature policies in a human readable form

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

signature validation: process of verifying and confirming that a digital signature is valid

signature validation application: application that implements signature validation

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

signature verification: process of checking the cryptographic value of a signature using signature verification data

signature verification data: data, such as codes or public cryptographic keys, used for the purpose of verifying a signature

signature verification device: configured software or hardware used to implement the signature verification data

signature data object: data structure containing the digital signature value, signature attributes and other information

signer: entity being the creator of a digital signature

signing service: facility that coordinates and manages the process by which an end user, by use of a personal device, can remotely sign a document, or other information, using a signing key stored in the signing service remote from the user

signing service provider: provider of a signing service

subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

subordinate CA: certification authority whose certificate is signed by the root CA, or another subordinate CA

NOTE: A subordinate CA can be a CA that issues end user certificates or other subordinate CA certificates.

subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations

supervision system: system that allows for the supervision of trust service providers and the services they provide, for compliance with relevant requirements

technical expert: person who provides specific knowledge or expertise to the audit team

NOTE 1: Specific knowledge or expertise relates to the organization, the process or activity to be audited, or language or culture.

NOTE 2: A technical expert does not act as an auditor in the audit team.

time assertion: time-stamp token or an evidence record

(electronic) time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

time-stamp policy: named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements

NOTE: This is a specific type of trust service policy.

time-stamp token: data object defined in IETF RFC 3161 [i.13], representing a time-stamp

time-stamping authority: trust service provider which issues time-stamps using one or more time-stamping units

time-stamping service: trust service for issuing time-stamps

time-stamping unit: set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time

trust: firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context

NOTE: As defined in Recommendation ITU-T X.1252 [i.5].

trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

trust anchor information: at least the distinguished name of the trust anchor, the associated public key, the algorithm identifier, the public key parameters (if applicable), and any constrains on its use including a validity period

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

NOTE 1: Such trust services are typically but not necessarily using cryptographic techniques or involving confidential material.

NOTE 2: ETSI EN 319 401 [i.47] provides a more specific definition.

trust service policy: set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements

trust service practice statement: statement of the practices that a trust service provider employs in providing a trust service

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

trust service status list: form of a signed list as the basis for presentation of trust service status information

trust service status list provider: entity which establishes, maintains and publishes trust service status lists

NOTE: A trust service status list provider is also called a trust service status list issuer or a trust service status list scheme operator (TSLSO).

trust service token: physical or binary (logical) object generated or issued as a result of the use of a trust service

NOTE: Examples of binary trust service tokens are: certificates, CRLs, time-stamp tokens, OCSP responses. Physical tokens can be devices on which binary objects (tokens or credentials) are stored. Equally, a token can be the performance of an act and the generation of an electronic record, e.g. an insurance policy or share certificate.

EXAMPLE: Certificates, CRLs, time stamps, OCSP responses. Physical tokens can be devices on which binary objects (tokens or credentials) are stored. Equally, a token can be the performance of an act and the generation of an electronic record, e.g. an insurance policy or share certificate.

trusted execution environment: specific execution environment on the mobile or personal device that consists of software and possibly hardware to define a boundary between an internal secure and an external unsecure (operating system) execution environment

NOTE: See GlobalPlatform Device Technology - TEE System Architecture [i.40].

trusted list: list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation

NOTE: In the context of European Union Member States, as specified in Regulation (EU) No 910/2014 [i.2], it refers to an EU Member State list including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

In the context of non-EU countries or international organizations, it refers to a list meeting the requirements of the present document and providing assessment scheme based approval status information about trust services from trust service providers, for compliance with the relevant provisions of the applicable approval scheme and the relevant legislation.

trusted list provider: entity which establishes, maintains and publishes trusted lists

NOTE: A trusted list provider is also called a trusted list issuer or a trusted list scheme operator (TLSO).

trusted service manager: trusted logical component that implements one or more service management roles related to the provisioning, the life cycle management and the deletion of a mobile service

NOTE: The TSM can be integrated with a mobile signature service or a signing service or can be provided by an independent party.

trusted user interface: means to securely address user interaction for sensitive applications through the display, keyboard, microphone, etc.

TSA disclosure statement: set of statements about the policies and practices of a time-stamping authority that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements

TSA practice statement: statement of the practices that a time-stamping authority employs in issuing time-stamp

NOTE: This is a specific type of trust service practice statement.

TSA system: composition of IT products and components organized to support the provision of time-stamping services

UTC(k): time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns

NOTE: A list of UTC(k) laboratories is given in clause 1 of Circular T [i.12].

validation: process of verifying and confirming that a certificate or a digital signature is valid

validation constraint: criterion, applied by a signature validation application when validating a signature

NOTE: Validation constraints can be defined in a formal signature policy, can be given in configuration parameter files or implied by the behaviour of the signature validation application.

validation data: data that is used to validate a digital signature

validation service: system accessible via a communication network, which validates a digital signature

verifier: entity that wants to validate or verify a digital signature

voluntary accreditation: any permission, setting out rights and obligations specific to the provision of trust services, to be granted upon request by the trust service provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the trust service provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body

XAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 132-1 [i.21] or ETSI EN 319 132-2 [i.22]

ZIP: Format as specified in PKWARE® [i.34].

3.2 Abbreviations

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

NOTE: These abbreviations apply in the ETSI ESI European framework for standardization of signatures.

AARL	Attribute Authority Revocation List
AC	Attribute Certificate
ACA	Attribute Certification Authority
AE	Acquiring Entity
ANSI	American National Standards Institute
AP	Asia Pacific
ARL	Authority Revocation List
ASiC	Associated Signature Container
ASN	Abstract Syntax Notation
ASN.1	Abstract Syntax Notation One
ATSv2	Archive-Time-Stamp attribute
ATSv3	Archive-Time-Stamp-v3 attribute
B2B	Business to Business
B2C	Business to Consumer
BER	Basic Encoding Rules
BIPM	Bureau International des Poids et Mesures
BMP	Basic Multilingual Plane
BPMN	Business Process Modelling Notation

BRG	Baseline Requirements Guidelines
BSP	Business Scoping Parameter
BTSP	Best practices Time-Stamp Policy
C/S	Client/Server
CA	Certification Authority
CAB	Conformity Assessment Body
CAB Forum	CA/Browser Forum
CARL	Certification Authority Revocation List
CC	Common Criteria
CC	Country Code
CD	Commission Decision
CEN	Comité Européen de Normalisation
CER	Canonical Encoding Rules
CMS	Cryptographic Message Syntax
CP	Certificate Policy
CPS	Certification Practice Statement
CR	Carriage Return
CRL	Certificate Revocation List
CSP	Certification Service Provider
CV	Card Verifiable
DA	Driving Application
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DIT	Directory Information Tree
DN	Distinguished Name
DRBG	Deterministic Random Bit Generator
DRG	Deterministic Random Generator
DRNG	Deterministic Random Number Generator
DS	Digital Signature
DSA	Digital Signature Algorithm
DSS	Digital Signature Service
DSS	Document Security Store
DSS-X	OASIS Digital Signature Services-eXtended
DTBS	Data To Be Signed
DTBSF	Data To Be Signed Formatted
DTBSR	Data To Be Signed Representation
DTD	Document Type Definition
DVC	Domain Validation Certificate
DVCP	Domain Validation Certificate Policy
EA	European Cooperation for Accreditation
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EC	European Commission
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECGDSA	Elliptic Curve German Digital Signature Algorithm
EDS	Electronic Delivery Service
EEA	European Economic Area
EL	Greece

NOTE: Alpha 2 country code for Greece, ISO 3166-1 [i.15].

EN	European Standard
ENISA	European Union Agency for Network and Information Security
EPES	Explicit Policy-based Electronic Signature
ER	Evidence Record
ERS	Evidence Record Syntax
ESS	Enhanced Security Services
EU	European Union
EUMS	European Union Member States
EV	Extended Validation

EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
FTP	File Transfer Protocol
GAA	3GPP Generic Authentication Architecture
GCC	Gulf Cooperation Council
GMST	Greenwich Mean Sidereal Time
GMT	Greenwich Mean Time
Gov2B	Government to Business
Gov2C	Government to Consumer
GTC	General Terms & Conditions
HMSSP	Home MSSP
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IAF	International Accreditation Forum
ICC	Integrated Circuit Card
ICS	Implementation Conformance Statement
IdP	Identity Provider
IERS	International Earth Rotation and Reference System Service
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPR	Intellectual Property Rights
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KEA	Key Encipherment or Agreement
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
LF	Line Feed
LoA	Level of Assurance
LOTL	List Of Trusted Lists
LTV	Long Term Validation
MDP	Modification Detection and Prevention
MNO	Mobile Network Operator
MS	Member State
MSSP	Mobile Signature Service Provider
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
NFC	Near Field Communications
NIST	National Institute of Standards and Technology
NR	Non-Repudiation
NRNG	Non-deterministic Random Number Generator
OASIS	Organization for the Advancement of Structured Information Standards
OCF	Open Container Format
OCF	OEBPS Container Format
OCSP	Online Certificate Status Protocol
ODF	Open Document Format
OEBPS	Open eBook Publication Structure
OID	Object IDentifier
OJEU	Official Journal of the European Union
OVC	Organizational Validation Certificate
OVCP	Organizational Validation Certificate Policy
PC	Personal Computer
PDF	Portable Document Format
PDS	PKI Disclosure Statements
PER	Packed Encoding Rules
PIN	Personal Identification Number
PIV	Personal Identity
PKC	Public Key Certificate
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
POE	Proof Of Existence

PP	Protection Profile
PSES	Preservation Service for Electronic Signatures
PSS	Probabilistic Signature Scheme
PTC	Publicly-Trusted Certificate
QC	Qualified Certificate
QCP	Qualified Certificate Policy
QCP-l	Policy for EU qualified certificate issued to a legal person
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD
QCP-n	Policy for EU qualified certificate issued to a natural person
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
QCP-w	Policy for EU qualified certificate issued to a web site
QSCD	Qualified electronic Signature/Seal Creation Device
RA	Registration Authority
RE	Routing Entity
REM	Registered Electronic Mail
REM-MD	REM Management Domain
RFC	Request For Comments
RGS	Référentiel Général de Sécurité
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman algorithm
RTF	Rich Text Format
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAA	Signature Augmentation Application
SAML	Security Assertion Markup Language
SAPS	Signature Application Practice Statement
SAV	Signature Acceptance Validation
SCA	Signature Creation Application
SCD	Signature Creation Data
SCDev	Signature Creation Device
SCE	Signature Creation Environment
SCS	Signature Creation System
SCVP	Server-Based Certificate Validation Protocol
SD	Signer's Document
SDO	Signed Data Object
SDR	Signer's Document Representation
SE	Secure Element
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module (for a mobile phone)
SMS	Short Message Service
SP	NIST Special Publication
SPO	Service Provision Option
SSCD	Secure Signature Creation Device
SSI	SCDev/SCA interface
SSL	Secure Socket Layer
SSP	Signing Service Provider
SVA	Signature Validation Application
TA	Trust Anchor
TAB	TABulator
TAI	International Atomic Time
TC	Technical Committee
TDP	TL Distribution Point
TEE	Trusted Execution Environment
TL	Trusted List
TLS	Transport Layer Security
TLS/SSL	Transport Layer Security/Secure Socket Layer protocol
TLSO	Trusted List Scheme Operator
ToC	Table of Content
TR	Technical Report
TrST	Trust Service Token

TS	Technical Specification
TS	Trust Service
TSA	Time-Stamping Authority
TSL	Trust-service Status List
TSLSO	Trust service Status List Scheme Operator
TSM	Trusted Service Manager
TSP	Trust Service Provider
TST	Time-Stamp Token
TST_A	Time-Stamp Token applied in an archive level of CAdES signature or XAdES signature
$TST_{T\text{-}Level}$	Time-Stamp Token applied in a T-Level of CAdES signature or XAdES signature
TSU	Time-Stamping Unit
TUI	Trusted User Interface
UA	User Agent
UCF	Universal Container Format
UCS	Universal Character Set
UICC	Universal Integrated Circuit Card (also known as a SIM card)
UK	United Kingdom

NOTE: Alpha 2 country code for Great-Britain, ISO 3166-1 [i.15].

UML	Unified Modelling Language
UN	United Nations
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time
UTF	Unicode Transformation Format
VCI	Validation Context Initialization
VE	Verifying Entity
VRI	Validation Related Information
WWW	World Wide Web
WYSIWHBS	What You See Is What Has Been Signed
WYSIWYS	What You See IS What You Sign
XER	XML Encoding Rules
XHTML	eXtended HTML
XKISS	XML Key Information Service Specification
XKMS	W3C XML Key Management Specification
XML	eXtensible Markup Language
XMLDSIG	eXtensible Markup Language Digital SIGnature
XMP	Extensible Metadata Platform
XSLT	eXtensible Stylesheet Language Transformations

Annex A: Bibliography

- IETF RFC 6170: "Internet X.509 Public Key Infrastructure - Certificate Image".
- Recommendation ITU-R TF.460-5: "Standard-frequency and time-signal emissions".
- ISO/IEC 27001: "Information security management".
- Commission Decision CD 2009/767/EC as amended.
- Recommendation ITU-R TF.536-1: "Time-scale notations".
- ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Extended Containers".
- ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

History

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