ETSI TS 119 101 V1.1.1 (2016-03)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for applications for signature creation and signature validation

Reference
DTS/ESI-0019101

Keywords
e-commerce, electronic signature, security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

Copyright Notification

Contents

Intellectual Property Rights

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

Modal verbs terminology

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

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

Introduction

Several aspects are important to ensure trust in digital signatures. Their successful implementation in electronic processes requires standards for related services, processes, systems and products as well as guidance for conformity assessment of such services, processes, systems and products.

NOTE 1: Regulation (EU) No 910/2014 [i.1] defines the terms electronic signature, advanced electronic signature, qualified electronic signature, electronic seal, advanced electronic seal and qualified electronic seal. These electronic signatures and seals can be created using digital signature technology.

NOTE 2: When not stated otherwise in the present document, "signature" denotes "digital signature".

The different players and the environment of the signature creation, validation and augmentation follow rules to allow them to be trusted. The present document concentrates on policy and security requirements to consider when creating, validating and augmenting signature in a trustworthy manner, in particular within the context of applications for signature creation, signature validation and signature augmentation.

1 Scope

The present document provides general security and policy requirements for applications for signature creation, validation and augmentation.

The present document is primarily relevant to the following actors:

- Implementers and providers of applications for signature creation, signature validation and/or signature augmentation, who need to ensure that relevant requirements are covered.
- Actors that integrate applications for signature creation, signature validation and/or signature augmentation components with business process software (or use standalone software), who want to ensure proper functioning of the overall signature creation/validation/augmentation process and that the signature creation/validation is done in a sufficiently secure environment.

The present document is applicable to these actors, and their evaluators (for a self-evaluation or an evaluation by a third party) to have a list of criteria against which to check the implementation.

The requirements cover applications for signature creation, signature validation and/or signature augmentation, i.e. the implementation and provision of the Signature Creation/Validation/Augmentation Application modules (SCA/SVA/SAA), the driving application (DA), the communication between the SCA and the signature creation device (SCDev) and the environment in which the SCA/SVA/SAA is used. It also specifies user interface requirements, while the user interface can be part of the SCA/SVA/SAA or of the DA which calls the SCA/SVA/SAA. Any entity using SCA/SVA/SAA components in its business process acts as driving application.

The document covers:

- Legal driven policy requirements.
- Information security (management system) requirements.
- Signature creation, signature validation and signature augmentation processes requirements.
- Development and coding policy requirements.
- General requirements.

Protection Profiles (PP) for signature creation applications and signature validation applications are out of scope and are defined in the CEN standard "Protection Profiles for Signature Creation & Validation Applications" [i.9].

General requirements for trust service providers are provided in ETSI EN 319 401 [i.24]. Requirements for trust service providers providing signature creation or validation services are out of scope. Requirements on trust service providers providing signature creation services are to be defined in ETSI TS 119 431 [i.22], with CEN EN 419 241 [i.21] defining requirements for a remote signature creation device. Requirements on trust service providers providing signature validation services are to be defined in ETSI TS 119 441 [i.23].

2 References

2.1 Normative references

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

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

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

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

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

[i.2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.3] ISO/IEC 15504: "Information technology -- Process assessment".

[i.4] ISO/IEC 27000 series: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.5] ISO/IEC 27001: "Information technology -- Security techniques -- Information security management systems -- Requirements".

[i.6] ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security management".

[i.7] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.8] ETSI TS 119 102 (all parts): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures".

[i.9] CEN EN 419 111: " Protection Profiles for Signature Creation & Validation Applications".

NOTE: At the time of publishing of the present document, this document is not yet published.

[i.10] ETSI EN 319 122 (all parts): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures".

[i.11] ETSI EN 319 132 (all parts): "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures".

[i.12] ETSI EN 319 142 (all parts): "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures".

[i.13] ETSI EN 319 162 (all parts): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[i.14] ETSI TS 119 172 (all parts): "Electronic Signatures and Infrastructures (ESI); Signature Policies".

[i.15] ETSI TS 119 104 (all parts): "Electronic Signatures and Infrastructures (ESI); General requirements on Testing Conformance and Interoperability of Signature Creation and Validation".

[i.16] ETSI TS 119 124 (all parts): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures Testing Conformance and Interoperability".

[i.17] ETSI TS 119 134 (all parts): "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signature (XAdES) Testing Compliance & Interoperability".

[i.18] ETSI TS 119 144 (all parts): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature (PAdES) Testing Compliance & Interoperability".

[i.19] ETSI TS 119 164 (all parts): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) Testing Compliance & Interoperability".

[i.20] ETSI TS 119 174 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Signature Policies".

[i.21] CEN EN 419 241: "Security requirements for trustworthy systems supporting server signing".

[i.22] ETSI TS 119 431: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing AdES digital signature generation services".

NOTE: At the time of publishing of the present document, this document is not yet published.

[i.23] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing AdES digital signature validation services".

NOTE: At the time of publishing of the present document this document is not yet published.

[i.24] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.25] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.26] ETSI EN 319 412-5: " Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[i.27] ETSI EN 301 549: "Accessibility requirements suitable for public procurement of ICT products and services in Europe".

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.7] and the following apply:

NOTE: For the sake of readability, the following definitions are reproduced here below.

advanced electronic seal: As defined in Regulation (EU) No 910/2014 [i.1].

advanced electronic signature: As defined in Regulation (EU) No 910/2014 [i.1].

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

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

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

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

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

personal data: any information relating to an identified or identifiable natural person ('data subject')

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

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

signature class: set of signatures achieving a given functionality

NOTE 1: ETSI TS 119 102-1 [i.8] 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 system: overall system, consisting of the signature creation application and the signature creation device, that creates a digital signature

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.15] and [i.16], XAdES-B-LTA, XAdES-E-C [i.17] and [i.18], PAdES-B-T, PAdES-E-LTV [i.19] and [i.20] are examples of signature levels.

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

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

signature validation application: application that implements signature validation

NOTE: The signature validation application takes inputs from and provides validation results to a driving application.

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

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

signer: entity being the creator of a digital signature

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

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

trusted path: connection that provides integrity, authenticity and confidentiality of the data transmitted

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.7] and the following apply:

CA	Certification Authority
CRL	Certificate Revocation List
DA	Driving Application
DN	Distinguished Name
DTBS	Data to be Signed
DTBSR	Data To Be Signed Representation
EC	European Commission
ICS	Implementation Conformance Statement
ISMS	Controls (Information Security Management System)
OCSP	Online Certificate Status Provider
OTP	One Time Password
PIN	Personal Identification Number
PUK	Personal Unblocking Key
PW	Password
SAA	Signature Augmentation Application
SAPS	Signature Application Practice Statement
SCA	Signature Creation Application
SCD	Signature Creation Data
SCDev	Signature Creation Device
SD	Signer's Document
SDO	Signed Data Object
SSI	SCDev/SCA interface
SVA	Signature Validation Application
ToC	Table of Content
XML	eXtensible Markup Language

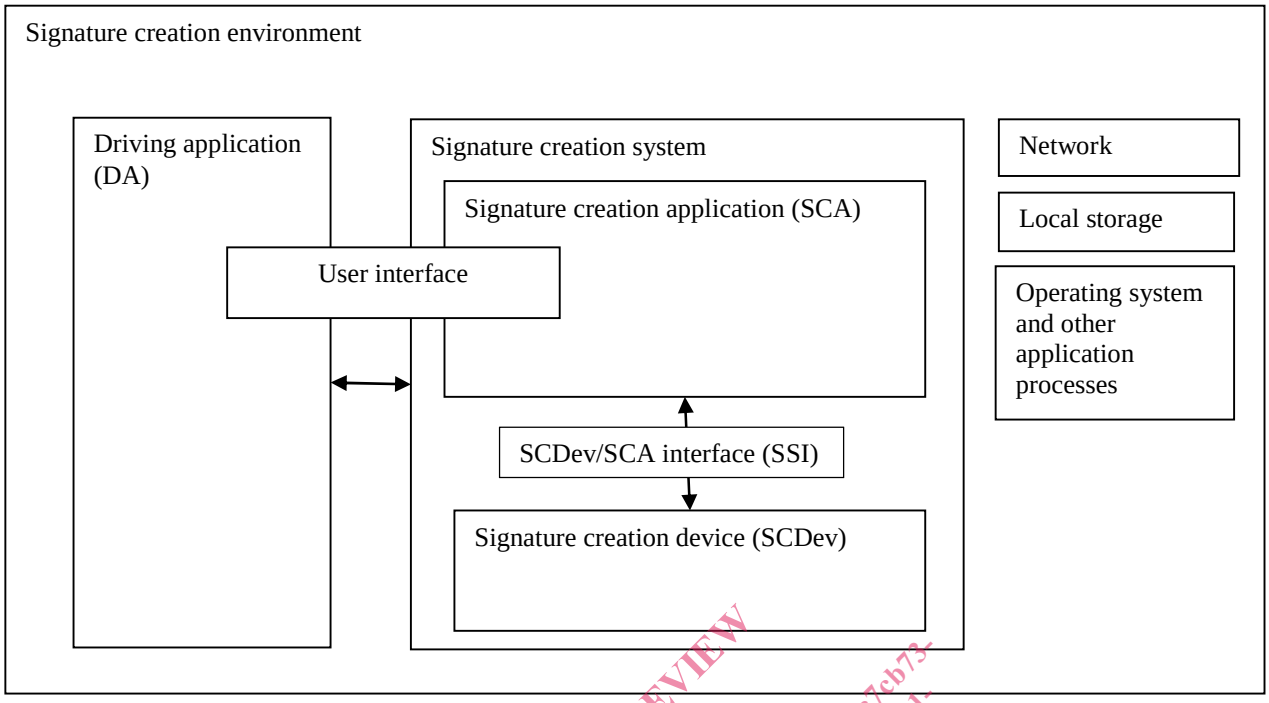
4 Signature creation/validation/augmentation model

The hardware/software systems for creating, validating or augmenting a signature, are modelled through several building blocks as shown in figures 1 to 3.

Some objectives can be implemented either by the DA or the SVA/SCA/SAA. This is to allow a flexibility in the implementation. However, a complete system meets all mandatory objectives (see clause 5.3) independent of where implemented.

NOTE 1: The distinction between the SCA/SVA/SAA and DA is done to simplify the definition of requirements. In concrete implementations, this distinction may not be made.

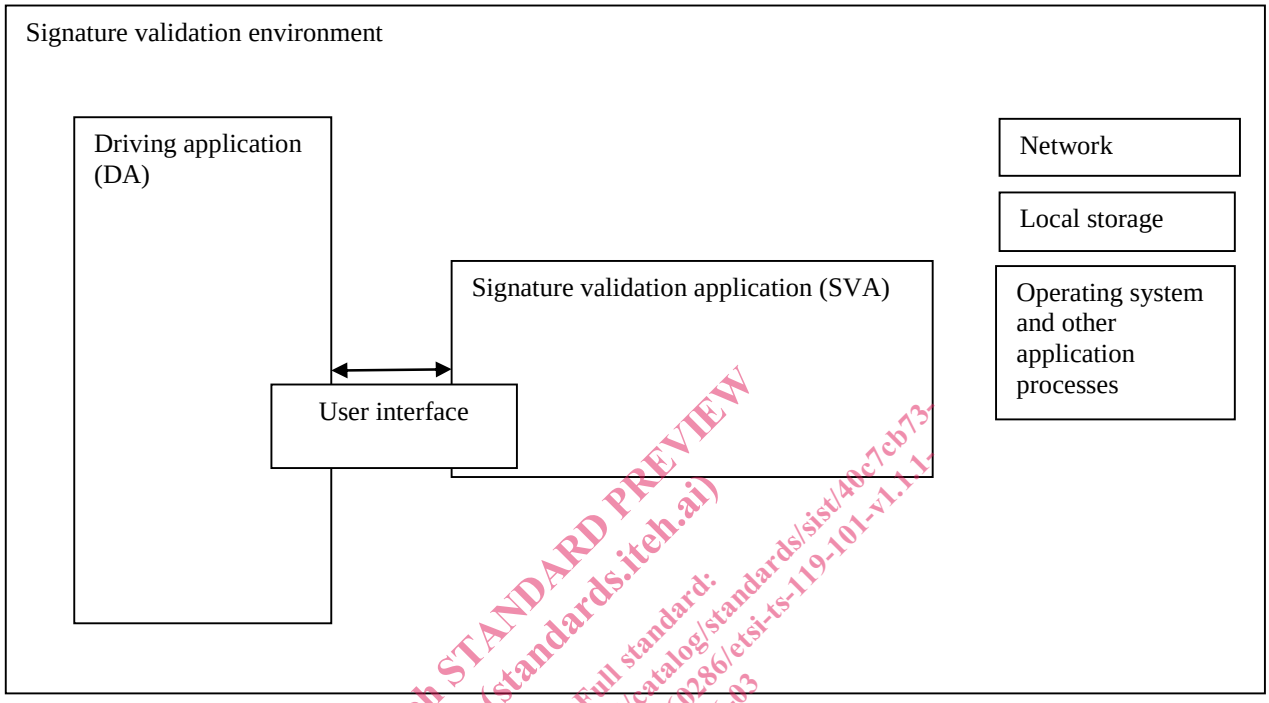
EXAMPLE: A SCA does not necessarily have a user interface, e.g. when signature creation is provided as a remote service. In this case user interaction, like selection of a signature creation policy, is implemented by the DA.



NOTE: This model is based on ETSI TS 119 102 [i.8] and differs slightly from the model used in CEN EN 419 111 [i.9]. It allows the user to communicate with the Driving Application and with the SCA. It also uses signature creation system to group together the SCA and the SCDev.

Figure 1: Basic model of an example signature creation environment

In case of a signature creation, the signature creation application (SCA) prepares the document to be signed and creates the signed data object from the digital signature value received from the signature creation device (SCDev). The digital signature value is created using the signature creation data of the user. The SCA communicates with the SCDev using the SSI. The driving application provides the input to the signature creation application and receives the output. The user interface can be (partly) part of the DA and/or (partly) part of the SCA. The signature creation environment covers the environment in which the DA, the SCA and the SCDev are used. It contains network, data storage and the information system.



NOTE: This model is based on ETSI TS 119 102 [i.8] and differs slightly from the model used in CEN EN 419 111 [i.9]. It allows the user to communicate with the Driving Application and with the SCA.

Figure 2: Basic model of an example signature validation environment

In the case of a signature validation, the DA provides the input for the SVA and receives the output. Again, the user interface can be part of the DA and/or part of the SVA. The signature validation environment covers the environment in which the DA and the SVA are used. It contains network, data storage and the information system.