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

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

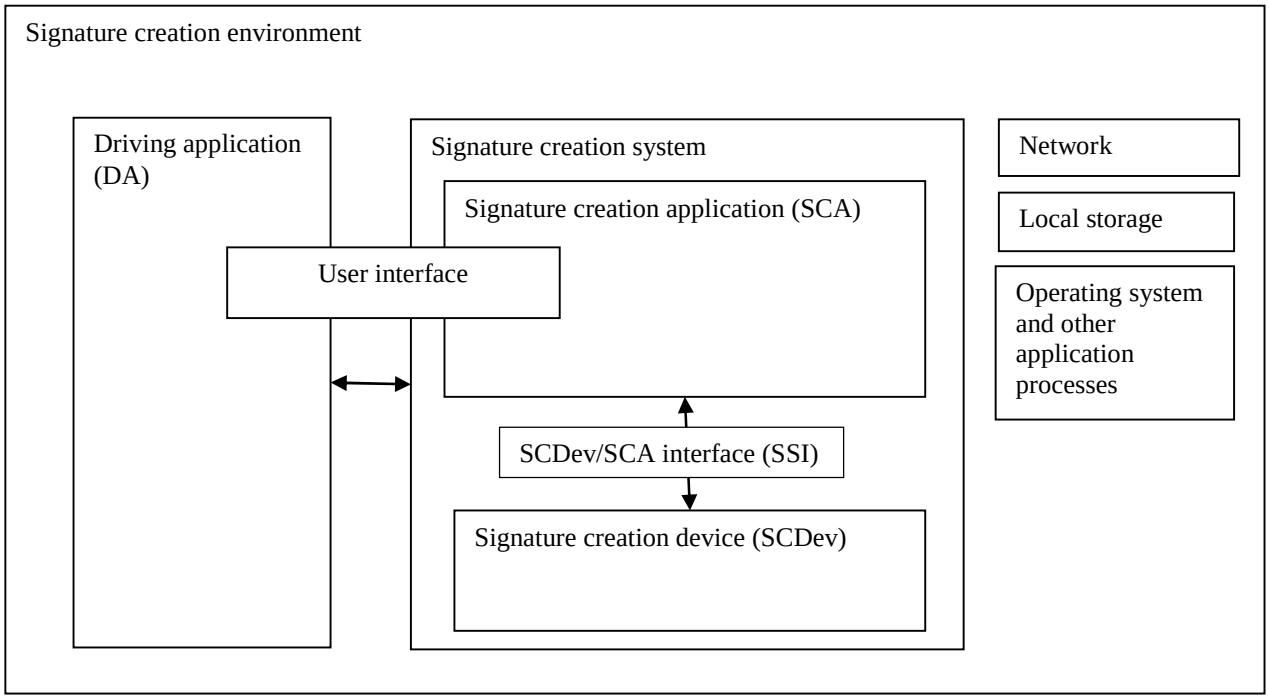
4 Signature creation/validation/augmentation model

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.

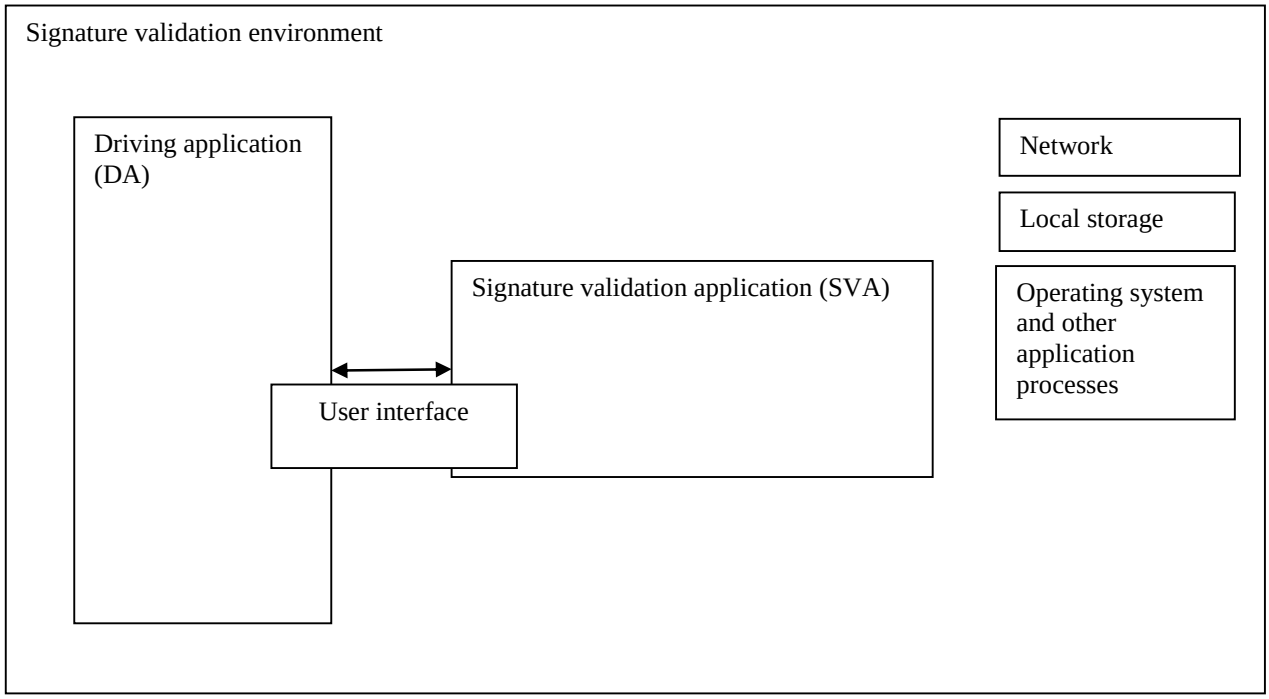
EXAMPLE: A SCA does not necessarily have a user interface, e.g. when signature creation is provided as a remote service. In this case user interaction, like selection of a signature creation policy, is implemented by the DA.



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.

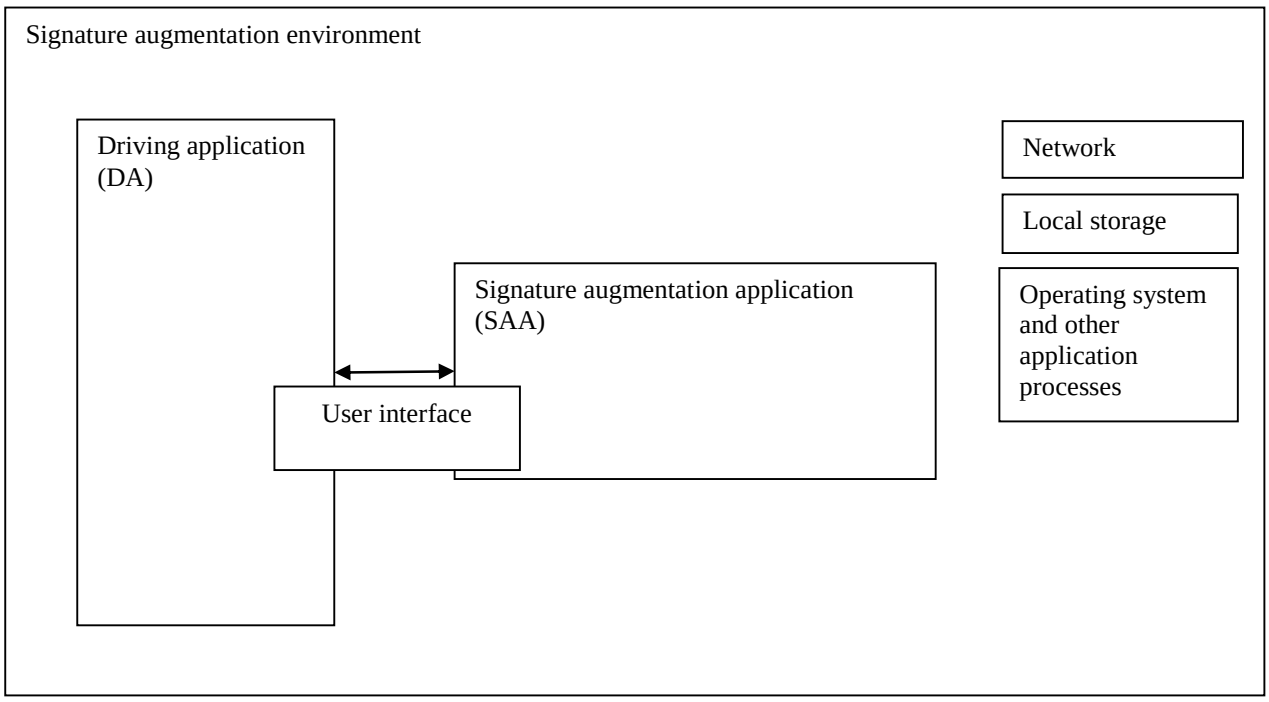


Figure 3: Basic model of an example signature augmentation environment

NOTE 2: In ETSI TS 119 102-1 [i.8], the signature augmentation is part of the SCA, since it adds information to the signature. In the present document it is handled separately to better cover the specific control objectives and to reflect the fact that the SAA can be part of the SCA, the SVA or can be a stand-alone application.

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

For more details on the general model for signature creation and validation, see ETSI TS 119 102 [i.8].

5 General requirements

5.1 User interface

Control Objective

Ensure that the user interface is well designed and easy to use to avoid any problems and misunderstandings in the interaction with the application. This ensures the user confidence. The user interface can be part of the SCA/SVA/SAA or the DA which calls the SCA/SVA/SAA.

Controls (User Interface)

UI 1: The user interface should:

a) provide unambiguous user guidance on how to use the SCA/SVA/SAA, and, if applicable, to install and configure the system;

b) be self-descriptive to the extent that each dialogue step is easy to understand through feedback from the system or is explained to the user upon request;

c) be error tolerant if, despite evident errors in input, the intended result can be achieved with minimal corrective action;

d) deliver informative error reporting to lead the user forward;

e) provide feedback to confirm that the action carried out by the user is correct (or incorrect);

f) when using colour indication, use red for errors and green for go/proceed;

g) be able, at any time, to cancel the current operation and return to the main menu; or, to exit the system completely;

h) protect privacy for the individual, e.g. by making the information not accessible to others at the user interface; and

i) ask for confirmation of the key decisions and choices of the user.

Control Objective

Provide the user with sufficient information to understand the process of generating, augmenting and validating the signature.

Controls (User Interface)

UI 2: The SCA/SVA/SAA shall provide a detailed user's guide leading first time users through the process of generating, augmenting and validating a signature.

5.2 General security measures

Control objective

Ensure that the systems on which the application is developed apply appropriate security measures and adapt to specific application environments.

Controls (General Security Measures)

GSM 1: Appropriate security measures:

GSM 1.1: The security measures for the systems on which the application is developed should be as in ISO/IEC 27002 [i.6] or based on a detailed risk analysis. Specific points of attention are listed below.

GSM 1.2: The latest application environment (managed software environments) should be used including up to date security fixes.

GSM 1.3: Well-tested and reviewed implementations of standardized protocol(s) and libraries shall be used.

GSM 1.4: Cryptographic libraries tested against the corresponding standard shall be used. Established libraries should be used.

GSM 1.6: If applicable, anti-virus, spyware protection (incl. for application parts that could be downloadable) shall be implemented.

GSM 1.7: If applicable, personal firewall shall be used.

GSM 2: Specific application environment:

GSM 2.1: When the SCA, SVA or SAA is delivered as a software package, it should be digitally signed.

GSM 2.2: When the delivered code or part of it is digitally signed, this should be done using a code-signing certificate provided by a recognized trust service provider issuing certificates and the signature should contain a time-stamp from a recognized time-stamping authority.

NOTE 1: Recognized according to the applicable code signing signature policy.

GSM 2.3: The DA should maintain integrity and confidentiality of all information supplied by the user and of any data flowing between the application and the user, even in the case of a public application environment.

GSM 2.4: The SCA/SVA/SAA shall maintain integrity and confidentiality of all information supplied by the user and of any data flowing between the application and the user, even in the case of a public application environment.

GSM 2.5: Signer's authentication data shall be securely deleted at the session end by the application to avoid any replay attack of other users.

GSM 2.6: If the application is used by different users, then the application shall make sure that all data related to a signature process is erased from public available areas (including caching, or certificates stores) after having completed the signature. The application shall not copy these elements to any party not authorized by the user.

NOTE 2: Security measures specific to the environment in which the SCA/SVA/SAA is used can be a result of a risk analysis done by the information security management system, see clause 7.

Control objective

Inform the user on recommended security measures when applying a SCA/SVA/SAA.

Controls (General Security Measures)

GSM 3: The SCA/SVA/SAA should inform the user of best practices in protecting personal computers (anti-virus, personal firewall, etc.).

NOTE 3: The corresponding information can be part of the SCA/SVA/SAA documentation.

5.3 System completeness requirements

Control objective

Ensure that a complete system implements all the mandatory requirements including those that can be implemented either by the DA or by the SVA/SCA/SAA.

Controls (System Completeness)

SC 1: In a complete system, all mandatory requirements stated in the present document shall be implemented.

6 Legal driven policy requirements

6.1 Introduction

When analysing the context of the business application implementing signatures, several legal aspects are considered. In the following clauses, control objectives are defined in connection with the processing of personal data and the accessibility for persons with disabilities.

6.2 Processing of personal data

Control objective

Ensure that personal data are processed fairly and lawfully in accordance with applicable personal data protection legislation.

Controls (Personal Data)

PD 1: Evidence shall be provided on how requirements of applicable Privacy and Data Protection regulation legislation (e.g. European Data Protection Directive [i.2]) are met.

PD 2: Appropriate technical measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

6.3 Accessibility for persons with disabilities

Control objective

Ensure that SCA/SVA/SAA are accessible for persons with disabilities.

Controls (Accessibility for Persons with Disabilities)

APD 1: If accessibility for persons with disabilities is required by applicable law, SCA/SVA/SAA shall be made accessible for persons with disabilities where feasible. Applicable standards such as ETSI EN 301 549 [i.27] should be taken into account.

EXAMPLE: Regulation (EU) No 910/2014 [i.1] states that where feasible, accessibility for persons with disabilities is required to be taken into account.

7 Information security (management system) requirements

7.1 Introduction

This clause contains the most important requirements for information security and information security management systems. A detailed description can also be found in the ISO/IEC 27000 series [i.4]. The controls defined in this clause cover the environment in which the SCA/SVA/SAA and the driving applications are applied.

ISMS 1: The controls identified in this cause shall be applied in the context of the organization information security management system.

ISMS 2: For an organization integrating signature creation and validation processes, information security should be implemented based on ISO/IEC 27001 [i.5], duly integrated with the following provisions.

7.2 Network protection

Control objective

If the SCA/SVA/SAA receives or sends confidential data over a network, guarantee the protection of this data in networks as well as the protection against network threats on the infrastructure supporting the processing and storage of confidential data.

Controls (Network Protection)

NP 1: If the SCA/SVA/SAA is implemented within an application environment containing components of different levels of security which communicate over networks, then the networks that transmit confidential data to or from the SCA/SVA/SAA should be adequately segmented to prohibit direct access from less trusted systems to higher trusted systems that contain or process confidential data. Confidential data should not be transmitted over uncontrolled or unprotected networks.

NP 2: Network access to information systems storing or processing confidential data shall be adequately restricted using filtering devices such as firewalls. Rules shall protect the information systems from both unauthorized incoming and outgoing traffic.

7.3 Information systems protection

Control objective

Ensure that the information systems handling signature data and the environment of the SCA/SVA/SAA are secured against unauthorized access and misuse, trigger suitable security alarms, and, when applicable, that security events are recorded.

Controls (information system protection)

ISP 1: Information systems shall be protected against malicious use with mechanisms such as anti-virus and anti-spyware or other prevention mechanisms.

ISP 2: If the SCA/SVA/SAA runs on an information system for several users, then an adequate access control mechanism shall prevent any unauthorized access to confidential data.

ISP 3: Security patches and fixes should be followed-up on a continuous basis.

ISP 4: Patch installations should be prioritized such that security patches for critical or at-risk systems are installed as soon as possible and within 30 days of the availability of the patches, and other lower-risk patches are installed within 90 days.

ISP 5: A security patch needs not be applied if it would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. The reason for not applying any security patches should be documented.

7.4 Software integrity of the application

Control objective

Ensure that integrity of the SCA, SVA, SAA and DA is properly protected.

Controls (Software Integrity of the Application)

SIA 1: SCA/SVA/SAA/DA components shall be protected against viruses and malicious software to ensure their integrity.

SIA 2: A change-detection mechanism (for example, file-integrity monitoring tools) shall be deployed to detect unauthorized modification (including changes, additions, and deletions) of critical SCA/SVA/SAA/DA components, like for example configuration files.

SIA 3: SCA/SVA/SAADA components that have been subject to viruses or malicious software attack shall be repaired or disabled until repair is possible.

SIA 4: If software components of the SCA, SVA, SAA or DA are intended to be published or delivered, these components shall be securely delivered, installed and configured.

7.5 Data storage security

Control objective

Ensure that appropriate data storage security measures are implemented in the SCA/SVA/SAA as well as in the application environment to protect any confidential data.

Controls (Data Storage Security)

DSS 1: Information systems storing confidential data should be configured according to a predefined security baseline based on a risk assessment.

DSS 2: Confidential data shall be protected against unauthorized access and unauthorized or unintentional changes and loss.

DSS 3: The SCA/SVA/SAA and its application environment shall support appropriate data storage security measures.

DSS 4: The data storage security measures introduced in DSS 3 should be as defined in ISO/IEC 27002 [i.6] or based on a detailed risk analysis.

7.6 Event logs

Control objective

To prove the activities related to the signature creation and validation, use event logs in the SCA/SVA/SAA, the driving application or the application environment to capture information which might be needed for later evidences.

Controls (Event Logs)

EL 1: Information systems storing or processing event logs should be configured according to a predefined security baseline based on a risk assessment.

EL 2: Event logs shall be protected against unauthorized access, and unauthorized or unintentional tampering or deletion.

EL 3: The SCA/SVA/SAA shall:

a) log the needed events itself; or

b) provide the necessary data to the driving application.

EL 4: If the SCA/SVA/SAA does not log the needed event, the DA shall log them.

EL 5: Any signature creation shall be logged.

EL 6: Any signature validation should be logged.

EL 7: Event logs shall be marked with the time of the event.

EL 8: Event logs should include the type of the event, the event success or failure, and an identifier of the person and/or component responsible for such an event.

8 Signature creation, validation and augmentation processing requirements

8.1 Signature creation process and systems

8.1.1 General

This clause specifies security requirements and recommendations specific to the signature creation. It contains requirements for the SCA, the DA and the user interface. It builds on the definitions, models and technical introduction of ETSI TS 119 102 [i.8].

NOTE 1: Contrary to the model in ETSI TS 119 102, the SVA described in this clause only covers to provide the minimum data that will be needed by the SVA to validate the signature. The process of augmenting the signature is covered in clause 8.3.

NOTE 2: A signature creation policy can be used to specify requirements on the signature process, with respect to the application of signatures to documents and data to be signed in a particular context, business or application domain, community in order for these signatures to be considered as valid signatures. The specification of a signature creation policy is out of the scope of the present document, see ETSI TS 119 172 [i.14] for more details.

NOTE 3: Sole control on the signing key is not covered by a specific control objective but by a combination of individual controls within clause 8.1.

8.1.2 Main functionalities requirements

Control objective

Ensure that the main functionalities of the SCA are well documented.

Controls (Signature Creation Process)

SCP 1: The SCA documentation shall indicate:

a) All the signature formats (CAdES [i.10], XAdES [i.11], PAdES [i.12], ASiC [i.13]) and signature levels that are supported.

b) Optional elements and features that are supported and how they can be selected and controlled.

EXAMPLE: Examples for such optional elements and features are whether signatures can be detached/enveloped/enveloping signatures, parallel signatures or counter signatures.

SCP 2: The SCA shall be controlled to support the functionalities, as documented in SCP 1.

8.1.3 Data content type requirements

Control objective

Ensure that the signature format is appropriate for the document data type that is to be signed and conforms to any legal or business requirements applicable.

Controls (Signature Creation Process)

SCP 3: The SCA documentation shall specify the data content types the SCA supports and can present correctly.

SCP 4: The SCA shall be controlled to support the data content types as documented in SCP 3.

Control objective

Ensure that the verifier cannot misinterpret the SD because of e.g. lack of information on the type of data, wrong syntax or inaccurate presentation or because the user interface is unable to present the SD correctly.

Controls (Signature Creation Process)

SCP 5: The SCA shall allow the inclusion of the SD data content type either implicitly in the document or explicitly as an explicit signature attribute.

SCP 6: If a SD content type is included in the signature, the SCA shall be able to provide it to the signer.

SCP 7: The user interface should warn the signer if the SD does not conform to the syntax specified by the data content type of the SD and should allow the signer to abort the signature process.

NOTE 1: No requirement is defined to abort the signature process when the SD does not conform to the syntax as it depends on the business process who makes the decision of abortion.

SCP 8: The user interface should warn the signer against creating a signature of any SD that indicates that it is of a data content type which cannot be presented to the user by the user interface.

NOTE 2: There can be business processes in which the signer will not view the SD in details before the signature, e.g. in case of mass signing of invoices.

SCP 9: The user interface should warn the signer if it cannot accurately present all parts of the SD according to the data content type.

Control objective (Signature Creation Process)

Ensure that the signature is applied to the right SD.

Controls

SCP 10: The SCA shall allow the signer to identify exactly what the signature will cover.

NOTE 3: This is especially relevant when the signature covers only part of a given document.

SCP 11: The DA shall allow the signer to select the SD among available documents.

SCP 12: In the case the process includes human interaction, the user interface should present the SD to the signer.

SCP 13: When the SD was presented to the signer, the SCA shall ensure that the SD presented to the signer is the same as the one that will be signed in the signature process.

SCP 14: The DA shall ensure that the SD selected by the signer for signing is the same as the one provided to the SCA for the signature.

Control objective

Ensure that the signer does not un-knowingly sign other embedded signed data objects with non-valid signatures created by others and that the signer is able to know which signatures have been validated or left unverified.

Controls (Signature Creation Process)

SCP 15: If the SD to sign contains signed data objects and if a signature validation application is available, before creating the signature:

i) the DA or the SCA should validate the signed data objects using a SVA.

SCP 16: If validation of the signed data objects was done:

i) the DA or the SCA should inform the signer about each signature validation policy that has been used by the SVA to perform the validation;

ii) the DA or the SCA shall inform the user about validation results; and

iii) the DA or the SCA shall inform the user about which signatures have been validated or left invalidated.

SCP 17: If the SD to sign contains signed data objects and if no SVA is available or used, the SCA should inform the signer that other signed data objects are embedded in the SD. and that he should validate the embedded signature externally before signing the document.

Control objective

Ensure that the signer does not accidentally alter the SD.

Controls (Signature Creation Process)

SCP 18: The SCA shall prevent the signer from changing any part of the SD during the presentation process.

Control objective

Ensure that the SCA is provided with enough information to be able to accurately present the SD to the signer over a user interface. Where presentation of the SD is important (i.e. presentation is one of the means of conveying the semantics), the SD can be ambiguous if not ensured, and the signer can infer a meaning from the SD that is not intended by the signer.

NOTE 4: The inclusion of the data content type, (e.g. .doc, .xlsx, jpg, etc.) as a signed attribute can prevent for example attacks based on inserting html instructions in the DTBS that, when the data type is replaced with "html" lead to a completely different presentation.

Controls (Signature Creation Process)

SCP 19: The DA should include the data content type attribute in the selection of the attributes to be signed.

SCP 20: The SCA shall allow inclusion of a data content type attribute in the DTBS to ensure that the data type of the SD is unambiguous.

SCP 21: If the SD can be ambiguous due to insufficient information describing the structure and interpretation of its semantics, the DA should include the data content type attribute in the selection of attributes to be signed to ensure that only a single interpretation of the SD's semantics can be made.

SCP 22: If the DA requests the inclusion of the data content type, the SCA shall encode the data type of the document and shall protect it by the signature.

Control objective

Ensure that an SD holding hidden code capable of modifying the signed document presentation without affecting its cryptographic validity does not deceive the verifier and/or the signer.

Controls (Signature Creation Process)

SCP 23: If the SD data type is susceptible to host malware or hidden code capable to alter the SD presentation without affecting the signature, the DA or the SCA should inform the signer of this data type weakness.

SCP 24: The DA or the SCA should clearly report to the signer if the data to be signed cannot be presented to the signer at all or cannot be presented in a reliable manner.

NOTE 5: A possible way of avoiding any problems with hidden code or malware is the transformation of the document to a type not having this problem.

Control objective

Ensure that the signer does not unwillingly sign a content or a commitment.

Control (Signature Creation Process)

SCP 25: The SCA shall allow the signer to be informed about the content being signed.

SCP 26: The SCA shall allow the signer to be informed about any commitment type to be used in the signature.

8.1.4 Signature attribute requirements

Control objective

Ensure that the signature is applied to the right signature attributes and that the attributes are not altered accidentally or maliciously.

Controls (Signature Creation Process)

SCP 27: The user interface shall allow the signer to view the signature attributes. In particular, the signer shall be able to check the content of the following:

a) the signer's certificate, in particular the distinguished name (DN) of the subject and the DN of the issuer;

b) the SD data content type (if present);

c) the signature policy (if present); and

NOTE 1: The signature policy is generally represented in the signature attributes by means of a signature policy identifier and the hash value of the signature policy.

d) the commitment type (if present).

SCP 28: The SCA shall ensure that the signature attributes presented to the signer are the same as those that will be signed in the signature process.

SCP 29: The DA shall ensure that the signature attributes (if any) selected by the signer for signing are the same as those that will be given to the SCA.

SCP 30: The user interface should warn the signer if the attribute type allows the presence of any hidden text, macros or active code in the attribute, or of any detected hidden elements.

Control objective

Ensure that the right certificate is used for creating the signature and no signature is created using an expired certificate. If possible, ensure that the certificate is not revoked at the moment of the signature.

Controls (Signature Creation Process)

SCP 31: When more than one signing certificate is available to be used by the signer, the DA shall allow the signer to select the certificate to be used for creating the signature. The DA may provide a default selection for the user. If there is only a single choice possible, this step may be omitted.

SCP 32: The SCA shall obtain the identifier from the DA needed to use the signature creation data associated with the selected certificate for signing.

SCP 33: The user interface shall allow the signer to inspect at least the following components of the certificates selected for inclusion in the DTBS:

a) the distinguished name (DN) of the subject;

b) the serial number; and

c) the DN of the issuer.

SCP 34: The SCA shall verify the signing certificate validity period, and if the current time is found outside that period, the SCA shall prevent the signer from using the corresponding signature creation data (SCD).

SCP 35: The SCA should verify for the certificates in the certificate chain from the signing certificate up to, but not including, the trust anchor, the validity period, and if the time of signature is found outside that period, the SCA should prevent the signer from using the signature creation data corresponding to this chain.

NOTE 2: Due to the direct trust in the trust anchor it is not needed to verify its status.

SCP 36: If the SCA has (on-line) access to the revocation information of the certificate, it may verify the revocation status information of the certificates in the certificate chain from the signing certificate up to, but not including, the trust anchor. If the signing certificate is found revoked, it shall prevent the signer from using the corresponding signature creation data. If another certificate of the chain is found revoked, it shall warn the user and the SCA should prevent the signer from using the SCD corresponding to this chain.

Control objective

Ensure that the correct (reference to) or signing certificate and other attributes are indicated in the signature and that this information is protected against substitution attacks.

Controls (Signature Creation Process)

SCP 37: The SCA shall protect the reference to or copy of the signing certificate within the signature from undetected replacement after the signature has been created.

NOTE 3: This typically is realized by signing this data along with the document and by putting it in e.g. the authenticated attributes section of the signature format.

Control objective

Ensure that the signature contains all attributes necessary to the purpose of the signature according to the business requirements, if this is not already clear from the context and content of the SD. Ensure that the signer is aware of the purpose of its signature.

Controls (Signature Creation Process)

SCP 38: The SCA shall ensure that the commitment is appropriately encoded in the signature, if a specific commitment was selected by the DA, the SCA or the user.

SCP 39: If a commitment type will be included into the signature, the user interface shall present the commitment type to the user.

Control objective

The user should be able to know which signature creation policy is used in the signature process. In the case that the business process foresees different signature creation policies to be selected by the signer, ensure that the signer knows which signature creation policies are supported.

Control (Signature Creation Process)

SCP 40: When more than one signature creation policy is available the signer may select the policy among available ones. In this case the SVA or DA shall:

a) provide to the user the list of possible signatures creation policies;

b) inform the user of the content of the signatures creation policies; and

c) request the user to select one.

SCP 41: If the user does not select a specific policy or if there is no explicit signature creation policy a default signature creation policy may be applied.

SCP 42: The signer should be able to request the applied signature policy used.

Control objective

Ensure that the explicit signature creation policy used for creating the signature and/or signature policy recommended to be used for validation of the signature is conveyed to the relying parties, if this is needed by the business, legal or policy requirements.

NOTE 4: An explicit signature policy included into the signature, can be wider than just a signature creation policy, e.g. it can include a signature validation policy or a signature augmentation policy.

Controls (Signature Creation Process)

SCP 43: If an explicit signature policy is needed by business, legal or policy requirements, the DA shall provide such a signature policy to the SCA.

SCP 44: If an explicit signature policy is provided by the DA, the SCA shall include an unambiguous identification of the exact provided policy within the signature.

NOTE 5: This can be done using a hash of the policy.

SCP 45: If the signer selected a signature creation policy, the DA shall provide it to the SCA with no change.

8.1.5 Time and sequence

Control objective

Ensure that the signature creation process follows the foreseen sequence of events.

Controls (Signature Creation Process)

SCP 46: The SCA shall compute the signature only after the signer has given its consent on calculating the signature.

SCP 47: If the business process contains the presentation of the DTBS or the SD to the signer, **t**he SCA shall compute the signature only after the DTBS or SD was presented to the signer.

NOTE: In the case of bulk signing the signer may not get all the DTBS/SD presented.

SCP 48: If the signature creation policy requires the use of one or more signature time-stamps, the SCA shall request a time-stamp token after the signature has been created. If a time-stamp token cannot be acquired within a time-limit specified by the policy the signature creation process shall be aborted.

8.1.6 Signature invocation requirements

Control objective

Ensure that each signature generated is the result of an explicit signature invocation. The user interface can be part of the SCA and/or of the DA.

Controls (Signature Creation Process)

SCP 49: The user interface shall limit accidental invocation of the signature process by the signer.

SCP 50: The SCA shall ensure that the signature is applied with the intent of the signer.

SCP 51: If the expression of will is a goal of the signature, prior to initiation of the signature process, the user interface shall request the signer to perform a non-trivial signature invocation interaction with the SCA that is unlikely to occur accidentally.

EXAMPLE 1: An example for a non-trivial action is scrolling down to the end of the document to be signed before accepting the signature, and not just selecting "next".

SCP 52: The user interface shall convey clear information that a signature is going to be created.

SCP 53: The user interface should be able to provide advice and information on all aspects of the signature, e.g. on process and legal status, if such information is available.

Control objective

Prevent situations where the SCA and SCDev are in the state where the signer's authentication data has been provided and the signer remains inactive for long periods of time, e.g. where the signer has been distracted from signature processing and another unauthorized person might possibly be able to complete the signature process on a modified or substituted SDs and signature.

Controls (Signature Creation Process)

SCP 54: In the SCA, a limit shall be defined on the idle time the SCA neither interacts with the signer, nor is processing. If this time limit elapses, then the signer shall authenticate again to the SCDev.

Control objective

Prevent situations where a misguided signer can perform operations in a wrong way so that an attacker can capture confidential data (e.g. a PIN or a password that would lead to signer's impersonation).

Controls (Signature Creation Process)

SCP 55: The user interface shall be as straightforward as the application can implement, to prevent the signer from creating security loopholes.

EXAMPLE 2: If the dialog is not clear, the user can enter confidential data into fields which are not secured.

SCP 56: The user interface shall be cleared of signer's confidential data after a time limit sufficient to perform normal operations. The fields where the confidential data were presented shall be overridden by other "neutral" data, to prevent latent images.

8.1.7 Cryptographic algorithm choice

Control objective

Ensure that all algorithms involved in calculating any element of the signature are based on algorithms and key lengths that are appropriate for the business requirements.

Controls (Signature Creation Process)

SCP 57: If the implicit or explicit signature creation policy requires a specific signature creation suite, including the key length, the SCA shall use the specified algorithm.

SCP 58: If a signature creation policy is used, the SCA shall check that the policy indicates which cryptographic algorithms can be used. If the policy does not contain such information, the SCA should warn the user of this fact and which algorithm is used.

SCP 59: If no signature creation policy is used or the policy does not contain any requirements on the cryptographic algorithms, algorithms and key length corresponding to ETSI TS 119 312 [i.25] should be used.

NOTE: Information on suitable algorithms and the time for which they are considered being secure can be found in ETSI TS 119 312 [i.25].

8.1.8 Signer's authentication requirements

8.1.8.1 General requirements

Control objective

Ensure that only the legitimate SCDev user can request creation of a digital signature value.

Controls (Signature Creation Process)

SCP 60: For knowledge based signer authentication, the authentication data (e.g. PIN or password) should withstand practical guessing and brute force attacks.

SCP 61: When the signer's authentication data transits through the SCA, the SCA shall maintain the confidentiality and integrity of the authentication data and shall securely erase it as soon as it is no longer needed (e.g. they are substituted or the signer's enrolment is removed).

SCP 62: Where authentication data (like a PIN or a PW) is sent from an external input device (like a PIN pad or a keyboard), then the data transmission between the input device and the SCDev shall be done over a trusted path.

SCP 63: If allowed by the SCDev, a function for securely changing knowledge based signer authentication data should be provided.

SCP 64: When entering knowledge based authentication data, like a PW or a PIN, the feedback shall not reveal its value. This may be done by providing the feedback of a typed digit or character to the signer by an appropriate symbol or method that does not reveal more than one digit or character at a time and only during a short period of time. This should be done by a feedback that does not reveal the digit or character at all.

NOTE: This masking is not needed for entering an OTP, since it is used only once.

SCP 65: Neither the SCA nor the signer's authentication component shall prevent the management of PIN/PW by the SCDev. Therefore they shall:

a) handle PIN/PW of the maximum length allowed for by the SCDev; and

b) not prevent signers to modify their own PIN/PW at will.

SCP 66: When changing the PIN/PW, the SCA shall require the presentation of a new PIN/PW twice and check whether both presentations are identical before delivering the new PIN/PW to the SCDev. When possible, the SCA should avoid that the user reuses the last used PWs or PINs.

Control objective

Ensure that brute force attacks are countered, e.g. the number of retries is protected by a retry counter.

Controls (Signature Creation Process)

SCP 67: The SCDev shall be configured with a maximum number of allowed consecutive wrong signer's authentication data.

SCP 68: When the signer provides the wrong signer's authentication data and the maximum as defined in SCP 67 is not reached, an error response shall be provided to the signer and the signer should be allowed to make a new try. No information on the type of mistake shall be provided to the user.

SCP 69: When the signer provides the wrong signer's authentication data and the maximal number of consecutive wrong signer's authentication data, as defined in SCP 67, is reached, the SCDev shall block the signer's authentication method and shall inform the signer.

SCP 70: The number of unsuccessful comparisons with the signer's authentication data shall be recorded with a retry counter. The SCDev may also provide a means for resetting the retry counter to its initial value (e.g. by presenting a reset code, also referred as Personal Unblocking Key (PUK)).

Control objective

Make sure that it is not possible to observe the signer's authentication data (for example, PIN/PW or biometric data).

Controls (Signature Creation Process)

SCP 71: The user should be informed by the documentation of steps to be taken to keep the signer's authentication data secure, including ensuring that the user is not overlooked by persons or cameras.

SCP 72: It shall not be possible to copy the signer's authentication data from the input of the SCA.

SCP 73: In the case where the application is used in a public area, the keyboard used to key in the information into the SCA, shall:

a) be protected from spying and over the shoulder peering, and

b) not emit keying sounds different for each key.

8.1.8.2 Requirements for biometric authentication methods

Control objective

Ensure that it is made difficult or practically impossible to make an impersonation attack with fakes of the biometric features.

Controls (Signature Creation Process)

SCP 74: Environment requirements suitable to prevent attacks to biometric devices, such as submission of "fake" biometric elements (silicon fingers, usage of latent images, etc.) shall be in place, if biometric devices are used.

Control objective

Ensure that replay attacks are countered: if biometric methods based on potentially publicly known data (face, ear shape, or fingerprint) are used, then the signer's authentication data is protected to ensure authenticity, e.g. an attacker can get public biometric features such as face and fingerprint images and derive the signer's authentication data from it in order to misuse the SCDev.

Controls (Signature Creation Process)

SCP 75: If biometric devices are used, a trusted path, providing integrity, authenticity and confidentiality, shall be provided for the transmission of biometric data between the biometric sensor unit and the SCDev.

SCP 76: If biometric devices are used, biometric sensors shall protect the user's biometric identification data from being used in replay attacks.

Control objective

Ensure that it is made practically impossible at enrolment time to link a person to someone else's biometric template. E.g. malicious code could intercept the data of the person to be enrolled and link it to a biometric data belonging to a different person, to later on export this association that will be used by the impostor to impersonate the authentic user.

Controls (Signature Creation Process)

SCP 77: If biometric devices are used, biometric data association to the user should not occur outside a trusted path or the SCDev.

Control objective

Ensure that it is made practically impossible at authentication time to alter the result of the signer's authentication data verification. E.g. an attacker could intercept the reply of the authentication process, in order to either give a false positive response (to authenticate an unauthorized person) or to give negative response (to enact a denial of service attack).

Controls (Signature Creation Process)

SCP 78: If biometric devices are used, matching of biometric data should not occur inside the SCA.

8.1.9 DTBS preparation requirements

Control objective

Ensure that an attacker cannot provide the SCA with forged signature components and prevent the SCA from applying the entire signature components specific to the format chosen to achieve a given purpose.

Controls (Signature Creation Process)

SCP 79: The SCA shall verify the validity, authenticity and completeness of all the components obtained in order to produce the correct DTBS format selected by the signer.

SCP 80: The SCA should use only hash algorithms specified in ETSI TS 119 312 [i.25].

SCP 81: The SCA should use only signature suites specified in ETSI TS 119 312 [i.25].

8.1.10 DTBSR preparation

Control objective

Ensure that the data to be signed representation (DTBSR) is correctly composed.

Controls (Signature Creation Process)

SCP 82: The SCA shall select the signature attributes according to the applicable rules or selected implicit or explicit signature creation policy.

SCP 83: The SCA shall produce the correct data to be signed representation (DTBSR) for a signature.

SCP 84: The SCA shall compute the DTBSR according to the applicable rules or selected implicit or explicit signature creation policy, by formatting, encoding and hashing of the DTBS. The hashing may be done in the SCDev, the formatting and encoding shall always done by the SCA.

SCP 85: The SCA shall maintain the integrity of the DTBS when computing the DTBSR.

8.1.11 Signature creation device

Control objective

Ensure that the signature creation device used for creating a signature has the right legal and technical level according to the business requirements.

NOTE: A possible way to convey this information to the SCA is the signature creation policy.

Controls (Signature Creation Process)

SCP 86: If the implicit or explicit signature creation policy requires a specific type of signature creation device, and this type can be checked automatically, the SCA shall check that the signature creation device corresponds to the given requirements.

EXAMPLE: If a qualified signature creation device is required by the signature creation policy, the SCA can check the related QCStatement (ETSI EN 319 412-5 [i.26]) within the signer certificate.

Control objective

Ensure that the SCDev is used as intended.

Controls (Signature Creation Process)

SCP 87: If the documentation of the SCDev contains an operational guide or equivalent information on how to use the device, the usage of the SCDev shall take into account any applicable guidance.

8.1.12 SCDev/SCA interface (SSI) requirements

The signature creation device (SCDev)/SCA Interface is responsible for the connection between the SCDev and the SCA.

Control objective

Ensure that the communication between SCA and SCDev is protected.

Controls (Signature Creation Process)

SCP 88: The SSI component shall prevent data communicated over the interface to be observed or changed.

SCP 89: For the types of SCDev that the SSI component claims to support, the SSI component shall support all items relevant to the physical interface in the specified range or with its specified characteristics to ensure proper operation.

SCP 90: The SSI component shall select the correct SCDev functionality, if the platform, on which the SCDev functionality is implemented requires a selection.

SCP 91: The SSI component shall select the signing certificate and then the related signature creation data.

8.1.13 Bulk signing requirements

Control objective

Ensure that a bulk signature process is not less secure than a process where each document would be signed separately.

Ensure that no documents are signed that are not intended to be signed by the signer.

Controls (Signature Creation Process)

SCP 92: When bulk signing is supported, the SCA shall allow the signer to individually display any SD that is part of the bulk signature process.

SCP 93: When bulk signing is supported, the SCA shall ensure that a document that was not selected by the signer cannot be part of the bulk signature process.

SCP 94: When bulk signing is supported, the SCA should provide a report of a bulk signature process including a list of every SD included in the bulk signing.

8.2 Signature validation process

8.2.1 Introduction

The signature validation process validates a signature against a set of validation constraints. These constraints are expressed in a signature validation policy, be it implicit or explicit, which reflects business, legal and security policy requirements.

One or more signature validation policies that are adapted to the business requirements can be defined.

A signature validation is always based on an implicit or explicit signature validation policy. It can be defined using:

- a description of that policy using a syntax like text, XML or ASN.1; or
- a set of configuration parameters.

When the signature that is received contains a signature policy identifier the driving application (DA) can use the signature policy to determine which signature validation policy is appropriate, but can also decide that another signature validation policy is more appropriate.

When the signature that is received does not contain a signature policy identifier, then the DA provides the signature policy.

A signature validation application (SVA) receives signed data and other input from the DA, validates the signature against a set of validation constraints and outputs a validation report. This report consists of a main validation result accompanied by additional data items, providing the details of the technical validation of each of the tested constraints, in particular when an invalid or an indeterminate result is being returned.

The validation can have one of the following results:

- *TOTAL-PASSED*: The signature is considered technically valid;
- *TOTAL-FAILED*: The signature is not to be considered technically valid;
- *INDETERMINATE*: The available information is insufficient to ascertain the signature to be valid or invalid.

The report can include additional information (e.g. time of validation, explanations and other information to be displayed) that has been found relevant by the SVA and can be relevant for the driving application (DA) in interpreting the results (see ETSI TS 119 102 [i.8]).

Within a validation process, the signature verification consists of checking the cryptographic value of the digital signature value using signature verification data.

The conceptual model of signature validation is described in ETSI TS 119 102 [i.8].

8.2.2 Main functionalities requirements

Control objective

Ensure that the main functionalities of the SVA are well documented.

Controls (Signature Validation Process)

SVP 1: The SVA documentation shall contain a description of:

a) the supported signature/container formats (e.g. CAdES [i.10], XAdES [i.11], PAdES [i.12], ASiC [i.13], etc.);

b) the supported signature/container levels for validation as specified in CAdES [i.10], XAdES [i.11], PAdES [i.12], and ASiC [i.13]); and

c) any specific restrictions on the supported signatures/containers.

EXAMPLE: Examples for such restrictions might be that only attached signatures are supported, or that signatures containing elements from older version of a standard are not supported.

SVP 2: The SVA shall be controlled to support the functionalities, as documented in SVP 1.

8.2.3 Validation process rules

Control objective

A sound process for signature validation is defined and followed. Such a process establishes whether a signature is technically valid against a signature validation policy.

Controls (Signature Validation Process)

SVP 3: Process rules shall be described in the SVA documentation (at least by reference to a relevant document). They shall define a procedure to validate signatures. This validation procedure should consider the validation of "old" signatures, where certificates may have expired or may have been revoked or even where the usage period of cryptographic algorithms may have been exceeded.

SVP 4: The validation procedure described in ETSI TS 119 102 [i.8] or procedures providing the same results should be used.

SVP 5: SVA implementation shall be controlled against the signature validation procedures defined as per SVP 3.

SVP 6: When the signature validation policy and/or some additional constraints of the DA mandate that some specific elements within the signature need to be present and signed, e.g. a commitment type, then the SVA shall verify that these elements are indeed present and signed.

SVP 7: The SVA documentation shall contain which signature validation policy is used by default, if there is any, and which validation constants can be configured and how.

8.2.4 Validation policy

Control objective

If the signature that is received contains a signature policy identifier, then the DA can use the signature policy identifier to determine which signature validation policy to use, but can also decide that another signature policy is more appropriate. The selection of the implicit or explicit signature policy used for the validation is up to the DA and depends on the business process and the purpose of the validation. For the verifier, the fact that a signature validation policy different from the one contained in the signature is a useful information.

Controls (Signature Validation Process)

SVP 8: If the signature contains a policy OID which is different from the policy used by the validation, then the SVA shall provide this information to the DA.

SVP 9: If the signature contains a policy OID which is different from the policy used by the validation, then the user should be informed.

8.2.5 Validation user interface

Control objective

Depending on the business model, the constraints and inputs to the validation process can either be provided by the DA (e.g. a default policy or a policy selected amongst a set of supported policies, according to the context; in this case, the driving application is able to select the signature validation policy to be used and can be allowed to override some of the default parameters) or fully or partly by the user.

In the second case, the user interface allows the selection of a signature validation policy by the user. In some cases a validation policy can even be parameterized by the user, in this case the interface allows the user to parameterize the selected validation policy.

Controls (Signature Validation Process)

SVP 10: According to the legal and business requirements, the SVA shall allow the DA or the user to select

a) the SDO to verify and the SD to verify if it is not included in the SDO;

b) if the attributes of the SDO do not contain the certificate(s) needed, the certificate(s) to be used for the validation;

c) if the SDO contains multiple signatures, the specific signature to be verified; and

d) the implicit or explicit signature validation policy to be used amongst the available ones.

SVP 11: The SVA may allow the user to provide further inputs for the validation process (i.e. elements to parameterize the validation policy such as the term of preservation, a trust anchor, etc.). This latter option should only be proposed in business contexts where the user has some notions of validation policies.

Control objective

Ensure that the user interface provides the result of the verification in a clear way to the user, if a user interface is part of the application.

Controls (Signature Validation Process)

SVP 12: The user interface shall be able to present, upon request from the user, a summary of the validation result to the user in a human readable form and shall be able to provide a validation report as per SVP 22.

SVP 13: The user interface shall be able to present the purported signer's identity, including:

a) the signer's certificate subject's distinguished name;

b) the distinguished name of the issuing CA; and

c) the distinguished name of the hierarchically superior CAs up to a root that is acceptable for the signature validation policy.

8.2.6 Validation inputs and outputs

Control objective

Ensure that:

- During the validation of a signature, the inputs required by the processing rules, the applicable signature validation policy, validation data (e.g. certificates, CRLs and OCSP responses) and a time-source are present and that all checks required by the verifier's signature validation policy are implemented.
- The validation process implemented provides the output status and output data as requested by the DA which presents the validation report.

NOTE 1: The output status and the output data can be presented either by the DA or by the SVA.

Controls (Signature Validation Process)

1. Inputs

SVP 14: The DA shall provide the signature to the SVA.

SVP 15: If the signature does not contain the signed document, the DA shall provide the signed document to the SVA.

SVP 16: The DA shall provide to the SVA the signature validation policy to be used in the validation process.

SVP 17: The SVA shall use in the signature validation process any applicable rules defined in the signature validation policy.

SVP 18: The DA or the SVA shall fetch the validation data as necessary using both the rules defined in the signature validation policy in the validation process and the pointers present in already fetched validation data.

SVP 19: The SVA shall have a reference time-source available.

2. Outputs

SVP 20: The SVA shall provide to the DA: the main validation result (valid, invalid, indeterminate), the time of validation and if requested a validation report.

SVP 21: The SVA shall provide further information about the elements of signature validation that pass or fail and additional information relating to the signature validation (certificates, revocation information, and time-stamps).

SVP 22: The user interface shall be able to present to the verifier the main validation results.

SVP 23: The user interface shall allow the user to learn:

a) the signature policy used in the signature validation;

NOTE 2: The validation always uses a signature policy, even if it is not explicitly specified by a signature policy identifier. An example of implicit signature policy is the applicable law.

b) when an explicit signature policy is used, the content or reference to this signature policy;

c) the name of the signer; and

d) any known commitment implied by the signature.

8.3 Signature augmentation process

8.3.1 Introduction

Augmenting signatures is 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.

A Signature Augmentation Application (SAA) receives signatures as well as other inputs from a driving application (DA) and augments a received signatures according to a set of constraints and outputs an augmentation report, optionally with an augmented signature.
The augmentation report shall indicate one of the three following results based on the signature augmentation policy:

successful: the signature has been successfully augmented.

augmentation unnecessary: the signature has not been augmented since the input signature is already compliant with the requirements of the signature augmentation policy.

EXAMPLE: Implicit or explicit augmentation policy requires signature with time and the signature already contains a signature time-stamp.

unsuccessful: the signature could not be successfully augmented.

The augmentation report consists of a main augmentation result accompanied by additional data items, in particular when an unsuccessful result is being returned. The format of the augmentation report is out of scope of the present document.

A signature augmentation process can be used in addition to a signature creation process, in addition to a signature validation process or independently of any signature creation process or signature validation process. The three cases are further addressed in the next clause.

8.3.2 The three use cases

8.3.2.1 Signature augmentation process used by a SCA

A SCA provides to verifiers at least a Basic Signature as defined in ETSI TS 119 102 [i.8], so that it can be validated against a signature validation policy.

However, if the SCA has an on-line access, it can provide more than this minimum format.

The SCA can thus apply, in addition to a signature creation policy, a signature augmentation policy.

EXAMPLE 1: It can provide, in accordance with a signature augmentation policy, a time-stamp token that will be applied to the signature. This allows to maintain the validity of a signature in case the signing certificate is revoked after the UTC time that is indicated within that time-stamp token.

EXAMPLE 2: It can include validation data (e.g. certificates, CRLs or OCSP responses), according to a validation policy, that can avoid a verifier to fetch this data.

8.3.2.2 Signature augmentation process used by a SVA

A SVA validates signatures against a signature validation policy and indicates to verifiers whether a signature is valid, invalid or whether its status cannot be determined.

However, generally the SVA has an on-line access and thus can augment the received signature with validation data, if this is requested by the verifier and if the signature has been successfully checked as being valid. If it has a connection to a TSA, it can also include a new time-stamp token within the signature.

The SVA can thus apply, in addition to a signature validation policy, a signature augmentation policy.

8.3.2.3 Independent signature augmentation process

In this case, a Signature Augmentation Application (SAA) is used independently of a SCA or of a SVA and adds to the signature the data elements required by the signature augmentation policy.

This independent process can be useful for signatures that have already been successfully verified and that have been archived. This means that an independent SAA does not need to validate signatures. However, it can check which cryptographic algorithms and hash functions are being used in a signature that is eligible to be augmented as well as the validity of the last applied time-stamp token to determine when the signature needs to be augmented.

8.3.3 Main functionalities requirements

Control objective

Ensure that the main functionalities of the SVA are well documented.

Controls (Signature Augmentation Process)

SAP 1: The SAA documentation shall indicate:

a) all supported signature/container levels to which it can augment the signature/container; and

b) any restrictions that apply on the augmentation.

EXAMPLE: Examples for such restrictions are supported hash algorithms, or if augmentation of detached, or parallel signatures are supported.

SAP 2: The SAA shall be controlled to support the functionalities, as documented in SAP 1.

8.3.4 Augmentation procedures

Control objective

Ensure that sound procedures for signature augmentation are defined and followed.

Controls (Signature Augmentation Process)

SAP 3: The implemented signature augmentation procedures shall be described in the SAA documentation (at least by reference to a relevant document).

SAP 4: The augmentation procedures described in ETSI TS 119 102 [i.8] should be used.

SAP 5: SAA implementation shall be controlled against the signature augmentation procedures defined as per SAP 3.

8.3.5 Data inclusion

Control objective

Ensure that the signature contains all the necessary data after the augmentation of the signature.

Controls (Signature Augmentation Process)

SAP 6: If the signature creation time is required by the chosen level to which the signature is augmented, then the SAA shall capture a time assertion (e.g. time-stamp, time mark or evidence record) as soon as possible after starting the augmentation process to provide a point of time that can be used to compare with the dates of possible events (e.g. key compromise, revocation, expiry).

SAP 7: If required by the chosen signature level to which the signature is augmented, information on certificates and their revocation status for the whole certificate path from the signer's certificate up to a trusted CA's certificate, shall be included by the SAA in the signature and, when relevant, protected by a trusted time. When the verification of the certificate path is not possible, the SAA may continue with the cryptographic signature verification and include this information in the result delivered to the DA.

8.3.6 Validation of the input signature to the augmentation process

Control objective

Ensure that the input signature is validated before augmentation if required by the signature augmentation policy.

Controls (Signature Augmentation Process)

SAP 8: If required by the signature augmentation policy, the input signature shall be validated.

SAP 9: If the signatures was validated, the augmentation report shall include the validation result.

9 Development and coding policy requirements

9.1 Secure development methods and application security

Control objective

Ensure the usage of appropriate (software) development methodology, tools and the implementation of adequate security measures.

Controls (Security Development Methods)

SDM 1: Use of (software) development methodology.

The first set of requirements is related to the use and implementation of a software development methodology.

SDM 1.1: A description of the used and implemented software development methodology shall be available.

SDM 1.2: The implemented methodology should follow formal processes.

EXAMPLE: An example for process assessment for Information technology can be found in ISO/IEC 15504 [i.3].

SDM 1.3: Control procedures should be available and documented.

SDM 1.4: The implementation of the methodology should be controlled against existing and documented procedures.

SDM 2: Functional and technical specifications:

SDM 2.1: The code shall be verified according to its functional and technical specifications.

SDM 2.2: Code control procedures shall be available and documented.

SDM 2.3: The code implementing the functional and technical specifications shall be controlled against existing and documented procedures.

SDM 3: Up to date security fixes in the software development environment shall be used.

SDM 4: The security measures for the software development environment should be as in ISO/IEC 27002 [i.6] or based on a detailed risk analysis.

9.2 Testing conformance requirements

Control objective

Ensure implementations are compliant with the standards they implement.

Controls (Testing Conformance requirements)

TC 1: If conformance to a standard is stated, then the conformance of the application shall be tested as described in the specifications on conformance testing, if such specifications exist.

NOTE: For general overview and requirements on conformance testing and interoperability see ETSI TS 119 104 [i.15]. For the implementation of specific signature formats see the corresponding documents for the implemented formats: ETSI TS 119 124 [i.16] for CAdES, ETSI TS 119 134 [i.17] for XAdES, ETSI TS 119 144 [i.18] for PAdES and ETSI TS 119 164 [i.19] for ASiC. For the conformance testing and interoperability of signature policies see ETSI TS 119 174 [i.20].

TC 2: The applied conformance tests shall be recorded and controlled.

TC 2.1: A description of the used methodology for conformance testing shall be available.

TC 2.2: Conformance testing procedures should be available and documented.

TC 2.3: The implementation of the methodology should be controlled against existing and documented procedures, as defined in TC 2.2.

TC 2.4: An implementation conformance statement (ICS) shall be made available for every implementation claiming conformance to a set of standards.

TC 2.5: The ICS should contain the following information:

a) administrative information identifying the manufacturer and the implementation (e.g. product name and version number);

b) identification of the standards to which conformance is claimed, including version numbers (and any profiles, if applicable);

c) identify which optional features of the standards are supported, if any;

d) identify any implementation dependent limitations (ranges, sizes, etc.).

TC 2.6: Whenever a new product version is released, at least regression tests shall be performed, which ensure that compatibility is maintained.

10 Signature application practice statement

A signature application practice statement (SAPS) may be established. An SAPS may be used on its own to state the rules to be applied to conform to the security and policy requirements or as part of a signature policy as described in ETSI TS 119 172 [i.14].

When such a document is established, its table of content (ToC) shall comply with the requirements stated in annex A.

The numbering of the clauses of the table of content is provided as it shall appear in the SAPS by removing the starting "A.". Each clause shall appear except clause A.0. If the clause does not apply, "not applicable" shall be written after the clause title. The text provided in each clause of annex A specifies the expected content of each clause. This text shall not be copied in the SAPS.

The clause in the SAPS corresponding to clause A.2 shall describe a set of rules with regards to the practices used by the application and its environment to properly implement the generation, augmentation and/or validation of signatures. This clause shall include, either by reference or explicitly, the set of policy and security practices requirements that the SCA, SAA and/or the SVA will have to meet when generating, augmenting and/or validating signatures in compliance with the SAPS and the applicable signature policy. When an explicit set of policy and security practices requirements is chosen, the clause shall conform to the structure defined in clause A.2.

EXAMPLE 1: A community of users defines as part of a signature policy the applicable requirements with regards to those practices any application will have to meet in order to comply with the community signature policy.

EXAMPLE 2: A signature policy refers to an external set of practice statements that describes the practices used by an application that generates, validates or augments signatures according to several signature policies defined by several communities of users.

EXAMPLE 3: A signature policy is defined in the context of a specific legal context and defines a set of rules to create, validate or augment a signature meeting specific legal requirements (e.g. a qualified electronic signature as defined in the applicable European legislation framework) including specific requirements on signature creation applications (SCAs), signature validation applications (SVAs), and signature augmentation applications (SAAs) and their environments.

NOTE: A SAPS stating such signature application practice defining requirements or making statements on the way signature applications are meeting application level policy and security requirements when creating or validating signatures, whatever and independently of the type of signature and of the set of requirements ruling the creation or validation of a type of signature (i.e. the applied signature policy), can be compared to a signature policy like a certification practice statement can be compared to a certificate policy.

Annex A (normative): Table of content for signature application practice statement

A.0 The right to copy

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the SAPS proforma in this annex so that it can be used for its intended purposes and may further publish the completed SAPS.

A.1 Introduction

A.1.1 Overview

This clause shall provide a general introduction to the document being written. It shall provide a synopsis of the business or application domain and the specific business or application process to which the SAPS applies. Depending on the complexity and scope of the particular business or application process implementing signatures, a diagrammatic representation may be included.

A.1.2 Business or application domain

A.1.2.1 Scope and boundaries of SAPS

This clause shall describe the scope and boundaries of the business (application) domain in which the SAPS is suitable for use.

NOTE: The business (application) domain is any business or commercial transaction process(es), which can involve several actors/participants and/or multiple actions and which can require one or multiple signatures to give it effect.

EXAMPLE: This can range from a purely corporate internal process or set of processes, through a multi-party trading network whose parties can negotiate and agree on the applicable terms and rules, up to nationwide rules governing the use of signatures in eGovernment and eBusiness processes.

The SAPS may be applicable to one or several domains of applications (e.g. B2B, B2C, Gov2B, Gov2C, contractual, financial, medical/health, consumer transactions, e-notary services, etc.), whether mono-organization, corporate or cross-organizations, nationwide or cross-borders, horizontal or vertical (e.g. eProcurement, eInvoice, eHealth, eJustice, etc.).

A.1.2.2 Domain of applications

This clause shall further describe each domain of applications that is considered for the use of the SCA/SVA/SAA.

A.1.2.3 Transactional context

This clause shall provide additional information about the transactional context, when applicable.

EXAMPLE: Request for proposal, any form of offer, exchange of documents of certain specific types, draft of contractual terms and nature of those terms (e.g. contract, non-disclosure agreement, etc.), approval, any type of acknowledgement (e.g. of receipt, of delivery, of sending, etc.), documents requiring specific types of authorization (e.g. because of value, because of applicable law or legal requirements, etc.), etc.

A.1.3 SAPS distribution points

This clause shall provide information about where the SAPS is available (e.g. a URL or by email) and how a paper/hard copy can be made available.

A.1.4 SAPS issuer

This clause shall include the name of the organization that is issuing the SAPS.

When the SAPS is signed digitally, it shall also provide information identifying the digital certificate certifying the public key corresponding to the private key used by the SAPS issuer to digitally sign the SAPS.

A.1.5 SAPS administration

A.1.5.1 Organization administering the document

This clause shall include the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of the SAPS.

A.1.5.2 Contact person

When the contact point is a person, this clause shall include the:

- first name and last name;
- electronic mail address;
- telephone number; and
- fax number, if applicable, of the person.

In other cases, it shall include:

- a title or role;
- an electronic mail alias; and
- other generalized contact information.

This clause may state that its contact person, alone or in combination with others, is available to answer questions about the SAPS.

A.1.6 Definitions and acronyms

This clause shall contain a list or a reference to a list of definitions for defined terms used within the document, as well as a list or a reference to a list of acronyms and their meanings.

A.2 Signature creation/augmentation/validation application practice statements

A.2.1 General requirements

This clause shall contain other general requirements, control objectives and controls in connection with:

1) the user interface (as specified in clause 5.1);
2) general security measures (as specified in clause 5.2; and
3) system completeness (as specified in clause 5.3).

A.2.2 Legal driven policy requirements

This clause shall contain requirements, control objectives and controls in connection with:

1) the processing of personal data (as specified in clause 6.2); and
2) the accessibility to persons with disabilities (as specified in clause 6.3).

A.2.3 Information security (management system) requirements

This clause shall contain requirements, control objectives and controls in connection with information security and information security management systems, and in particular:

1) network protection (as specified in clause 7.2);
2) information system protection (as specified in clause 7.3);
3) software integrity of the application (as specified in clause 7.4);
4) data storage security (as specified in clause 7.5); and
5) event logs (as specified in clause 7.6).

A.2.4 Signature creation, signature validation and signature augmentation processes requirements

This clause shall contain requirements, control objectives and controls in connection with:

1) Signature creation process and systems, and in particular:
   a) main functionalities (as specified in clause 8.1.2);
   b) data content type management (as specified in clause 8.1.3);
   c) signature attributes (as specified in clause 8.1.4);
   d) timing and sequencing enforcement (as specified in clause 8.1.5);
   e) signature invocation (as specified in clause 8.1.6);
   f) cryptographic algorithm choice (as specified in clause 8.1.7);
   g) signer's authentication procedure (and access control management) (as specified in clause 8.1.8);
   h) DTBS preparation (as specified in clause 8.1.9);
   i) data to be signed representation (DTBSR) (as specified in clause 8.1.10);
   j) signature creation device management (as specified in clause 8.1.11);
   k) protection of the communication between SCDev and SCA (as specified in clause 8.1.12); and
   l) bulk signing operation (as specified in clause 8.1.13).
2) Signature validation process and systems, and in particular:
   a) main validation functionalities (as specified in clause 8.2.2);
   b) validation process rules enforcement (as specified in clause 8.2.3);
   c) validation policy (as specified in clause 8.2.4);
   d) validation user interface (as specified in clause 8.2.5); and
   e) validation input/output relative conformance (correctness of the implemented validation procedure) (as specified in clause 8.2.6).

3) Signature augmentation process and systems, and in particular:

   a) main augmentation functionalities (as specified in clause 8.3.3);

   b) augmentation process rules enforcement (as specified in clause 8.3.4);

   c) data inclusion during the augmentation (as specified in clause 8.3.5); and

   d) validation of the input signature (as specified in clause 8.3.6).

A.2.5 Development and coding policy requirements

This clause shall contain requirements, control objectives and controls in connection with the development and coding policies, in particular with:

1) the secure development methods (as specified in clause 9.1); and

2) testing conformance (as specified in clause 9.2).

Annex B (informative): Bibliography

- ISO 22301: "Societal security -- Business continuity management systems --- Requirements".
- ISO 22313: "Societal security -- Business continuity management systems -- Guidance".
- ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".
- ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation".

History

Document history		
V1.1.1	March 2016	Publication