ETSI TS 119 431-2 V1.1.1 (2018-12)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for trust service providers;
Part 2: TSP service components supporting AdES
digital signature creation

Reference
DTS/ESI-0019431-2

Keywords
electronic signature, security, trust services

ETSI

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

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

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

Important notice

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

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

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

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

The present document is part 2 of a multi-part deliverable covering Policy and security requirements for trust service providers, as identified below:

Part 1: "TSP service components operating a remote QSCD / SCDev";

Part 2: "TSP service components supporting AdES digital signature creation".

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.

Executive summary

The present document specifies policy and security requirements for TSP service components creating AdES digital signatures. The TSP service component relies either on remote server signing or on a signature creation device in the user's environment to create digital signature.

These requirements are based on the general policy requirements specified in ETSI EN 319 401 [9] and consider related requirements from ETSI TS 119 101 [1].

Introduction

The creation of digital signatures can involve different tasks provided by trust service providers. This can cover not only the creation and management of certificates as described in ETSI EN 319 411-1 [i.7] but also the management of signing keys as described in ETSI TS 119 431-1 [i.8] or the creation of the AdES digital signature as described in the present document.

The present document gives no restrictions on where signing key management is done. It can be handled either by a server signing application service component SSASC as described in ETSI TS 119 431-1 [i.8] or directly by the client in a signature creation device (SCDev).

1 Scope

The present document provides policy and security requirements for trust service providers (TSP) implementing a service component supporting AdES digital signature creation. This component contains a signature creation application and is thus called signature creation application service component (SCASC). However, it is more than just the SCA. It contains service elements around which parts of the driving application as defined in ETSI TS 119 102-1 [1] and ETSI TS 119 101 [2] can be implemented. The present document does not give restrictions on whether something is covered within a signature creation application or outside, as long as it is done by the SCASC.

The present document gives no restrictions on the type of TSP implementing such a service component.

The present document aims at supporting the creation of digital signatures in European and other regulatory frameworks.

NOTE 1: Specifically, but not exclusively, the present document is aimed at trust services, supporting the creation of digital signatures in accordance with the requirements of the Regulation (EU) No 910/2014 [i.1] for electronic signatures and electronic seals (both advanced and qualified). Annex B contains specific requirements for SCASC in the context of Regulation (EU) No 910/2014 which aim at providing best practice requirements for the creation of advanced electronic signatures and seals based on X.509 certificates.

NOTE 2: Specifically, but not exclusively, digital signatures in the present document can be used to create electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1].

The present document may be used by competent bodies as the basis for confirming that an organization is trustworthy in creating AdES digital signatures.

NOTE 3: See ETSI EN 319 403 [i.6] for guidance on assessment of TSP processes and services.

The SCASC has connections with external (trust) services that can be contacted for example for provisioning information to be included within the signature. The present document does not put requirements on the trust service policy applied by such external services.

The present document does not specify any protocol used to access the SCASC or how the SCACS can contact an SSASC or an SCDev.

NOTE 4: Protocols to contact a SCASC or a SSASC are defined in ETSI TS 119 432 [i.9].

The present document identifies specific controls needed to address specific risks associated with services providing AdES signature creation.

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.

[1] ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

[2] ETSI TS 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

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

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

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

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

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

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

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

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

[i.3] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents". .

[i.4] CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing; Part 1: General System Security Requirements".

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

[i.6] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.7] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.8] ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".

[i.9] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

3 Definition of terms, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.2] and the following apply:

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

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

remote signature creation device: signature creation device used remotely from signer perspective and provides control of signing operation on the signer's behalf

server signing application: application using a remote signature creation device to create a digital signature value on behalf of a signer

server signing application service component: TSP service component employing a server signing application

server signing application service provider: TSP operating a server signing application service component

signature applicability rules: set of rules, applicable to one or more digital signatures, that defines the requirements for determination of whether a signature is fit for a particular business or legal purpose

NOTE: Signature applicability rules can be implicit, or can be stated in a human readable document and/or in a machine processable from. ETSI TS 119 172-1 [i.3] can be used for this purpose.

signature creation application: application within the signature creation system that creates the AdES digital signature and relies on the SCDev to create a digital signature value

NOTE: The SCDev can be managed by the SSASC.

signature creation application service component: TSP service component employing a signature creation application

signature creation application service provider: TSP operating a signature creation application service component

signature creation constraint: criteria used when creating a digital signature

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

signature creation policy: set of **signature creation constraints** processed or to be processed by the SCA

signature creation service: TSP service implementing a signature creation application and/or a server signing application

signature creation service provider: service provider offering a signature creation service

NOTE: As in CEN EN 419 241-1 i.4.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 119 001 [i.2] and the following apply:

CA	Certification Authority
DTBS	Data To Be Signed
DTBSR	Data To Be Signed Representation
OID	Object IDentifier

QES	Qualified Electronic Signature or Qualified Electronic Seal
SAD	Signature Activation Data
SCA	Signature Creation Application
SCASC	Signature Creation Application Service Component
SCASP	Signature Creation Application Service Provider
SCDev	Signature Creation Device
SCS	Signature Creation Service
SCSP	Signature Creation Service Provider
SD	Signer's Document
SDO	Signed Data Object
SLA	Service-Level Agreement
SSA	Server Signing Application
SSASC	Server Signing Application Service Component
SSASP	Server signing application service provider
TSA	Time-Stamping Authority
URI	Uniform Resource Identifier

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any TSP conforming to the present document. Such requirements are indicated by clauses without any additional marking;

b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]".

The requirements in the present document are identified as follows:

<the 3 letters identifying the elements of services > - < the clause number> - <2 digit number - incremental>

The elements of services are:

- **OVR:** General requirement (requirement applicable to more than 1 component)
- **ASI**: AdES signing interface

The management of the requirement identifiers for subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
- The requirement identifier for deleted requirements are left and completed with "VOID".
- The requirement identifier for modified requirement are left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

4 General concepts

4.1 General policy requirements concepts

The present document is structured in line with ETSI EN 319 401 [9]. It incorporates ETSI EN 319 401 [9] requirements by reference and adds requirements relevant for a SCASP.

See ETSI EN 319 401 [9], clause 4 for guidance for guidance on general policy requirements.

4.2 Signature creation application service component applicable documentation

4.2.1 Signature creation application service component practice statement

The **signature creation application service provider (SCASP)** develops, implements, enforces, and updates a **SCASC practice statement** which is a trust service practice statement such as defined in ETSI EN 319 401 [9], instantiated for a signature creation application service component. See clause 6.1.

The SCASC practice statement describes ***how*** the SCASP operates its service and is owned by the SCASP. The SCASC practice is tailored to the organizational structure, operating procedures, facilities, and computing environment of a TSP. The recipients of the practice statement can be auditors, subscribers and relying parties.

NOTE: The presence of some elements is mandatory in the SCASC practice statement as requested in the present document, however the present document places no restriction on the form of the SCASC practice statement; it can be included in a general TSP practice statement document that covers other services delivered by that TSP or it can be a standalone document. Annex A provides a recommended table of content.

The present document provides requirements identified as necessary to support a high-level SCASC policy, to be endorsed by a SCASP and reflected in its **practice statement**.

4.2.2 Signature creation application service component policy

A **SCASC policy** describes **what** is offered and can contain diverse information beyond the scope of the present document to indicate the applicability of the service. A SCASC policy is defined independently of the specific details of the specific operating environment of a SSASP. The recipients of the service policy can be auditors, subscribers and relying parties.

The present document can be referred by such a SCASC policy to provide information about the level of the service.

SCASPs conforming to the present document's normative requirements except those defined in annex B may use in its documentation the following specific OID:

itu-t(0) identified-organization(4) etsi(0) CREATION SERVICE-policies(19431) ades (2) policy-identifiers(1) main (1)

SCASPs conforming to the present document's normative requirements including those defined in annex B may use in its documentation the following specific OID:

itu-t(0) identified-organization(4) etsi(0) CREATION SERVICE-policies(19431) ades (2) policy-identifiers(1) eu-advanced-x509 (2)

A SCASC policy is not necessarily part of the SCASP's documentation (as per ETSI EN 319 401 [9] a practice statement and general terms and conditions are sufficient); e.g. a SCASC policy can be shared by a community and not owned by the SCASP. Also, the present document does not put constraints on the form of the SCASC policies; a SCASC policy can be a stand-alone document or be provided as part of the practice statements and/or the general terms and conditions.

The present document does not put any limitation on the content of the SCASC policies but it is requested that the SCASP provides minimal information about the service it offers (see clauses 6.1 and 6.2).

4.2.3 Terms and conditions

In addition to the SCASC practice statement and, when issued by the SCASP, the SCASC policy, the SCASP also issues terms and conditions, see clause 6.2. Terms and conditions can cover a broad range of commercial terms or technical terms that are not necessarily communicated to the customer, etc. The terms and conditions are specific to a SCASP. The recipients of the terms and conditions can be the subscribers and the relying parties.

NOTE: The presence of some elements is mandatory in the terms and conditions as requested in the present document, however the present document places no restriction on the form of terms and conditions; it can be a standalone document for a public audience, or it can be split over subscriber's agreement(s) and information to relying parties. The form and content of the terms and conditions can also depend on national regulations.

4.2.4 Other documents associated with signature creation

Besides the description of the practices employed by the SCASP to offer the AdES digital signature creation service, it is important to document the criteria under which the signatures are created and, beyond this, can then be determined as fitting a certain business need.

Two documents can be used for these purposes:

- A **signature creation policy** which is the set of **signature creation constraints** processed by the SCA. A signature creation policy can be identified by means of an OID;
- **Signature applicability rules** that can be structured as per ETSI TS 119 172-1 [i.3] and can include a signature creation policy containing the signature creation constraints to be applied by the SCA, as well as other criteria showing the applicability of the created signature so certain business needs.

NOTE: The use of signature applicability rules is outside the scope of the present document but can be applied as an extension to the signature creation service as covered by the present document.

The SCASC practice statement, the signature creation policy and the signature applicability rules are different types of documentation; the SCASC practices statement describe ***how*** the SCASP operates its service, while the signature creation policy *states the constraints* to be processed by a *SCA* when creating a signature. Going beyond the scope of a signature creation policy, the signature applicability rules *state the rules and assumptions* used by a *user* to decide whether a signature created according to these rules is *fit for purpose*.

The owner of the SCASC practice statement is a SCASP, while the owner of the signature applicability rules is usually the signatory.

4.3 Architecture

A TSP service component supporting AdES digital signature creation (SCASC) receives the document(s) and/or hash(es) of document(s) to be signed and optionally some signing parameters, collects all necessary information to create the signature, prepares the data-to-be-signed representation (DTBSR) and sends this to the SCDev. The SCDev can be either in the user's environment or managed by a remote server signing application service component (SSASC) as described in ETSI TS 119 431-1 [i.8]. For the purpose of the present document, it is assumed that the SCDev handles the authentication and the agreement to sign with the user and returns the digital signature value, without going into details if this is done by the SCDev itself or the component managing the SCDev. The authorization to use the signing key within the SCDev can go through the SCASC but can also be done directly by communication between the signer and the SCDev. The digital signature value is included by the SCASC into the digital signature.

NOTE: The SCASC represents the signature creation application in CEN EN 419 241-1 [i.4].

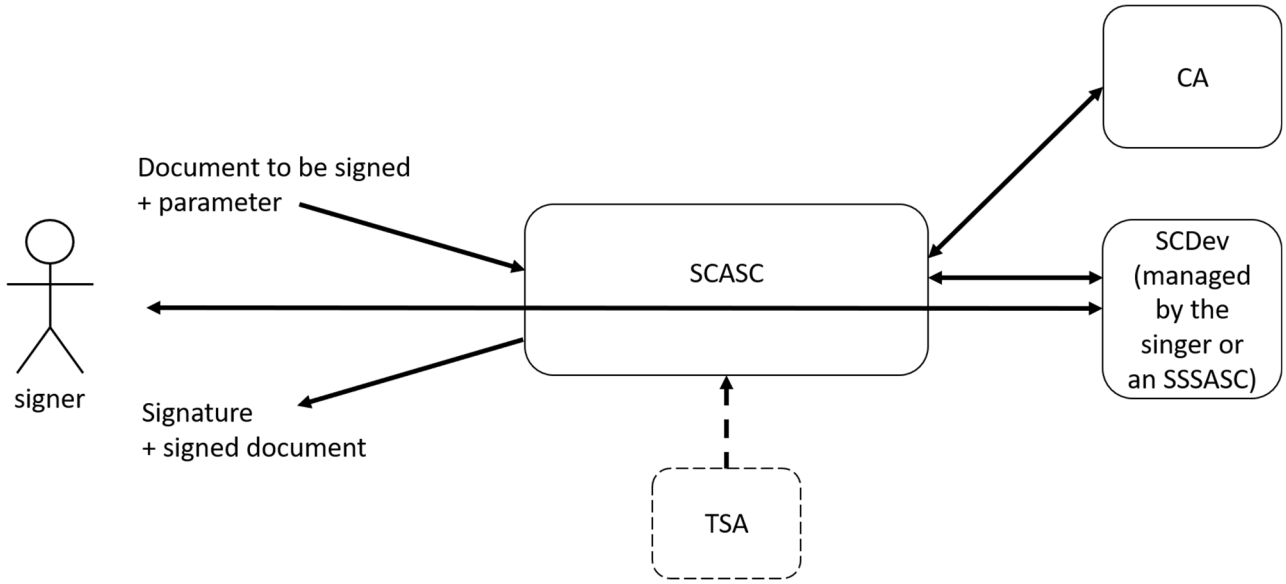

Figure 1: Relations of the TSP service component for AdES digital signature creation

5 Risk assessment

OVR-5-01: The requirements specified in ETSI EN 319 401 [9], clause 5 shall apply.

6 Policies and practices

6.1 Trust service practice statement

OVR-6.1-01: The requirements specified in ETSI EN 319 401 [9], clause 6.1 shall apply.

In addition, the following particular requirements apply:

OVR-6.1-02: [CONDITIONAL] When the SCASC supports the inclusion of time-stamp tokens in the AdES digital signature, the SCASC practice statement shall list which TSA are used.

OVR-6.1-03: The SCASC practice statement shall specify all the supported signature creation polices.

OVR-6.1-04: The SCASC practice statement shall specify all the supported signature formats.

OVR-6.1-05: The SCASC practice statement shall specify all the supported signature classes.

NOTE: ETSI TS 119 102-1 [2] describes different signature classes.

OVR-6.1-06: The SCASP shall identify in the SCASC practice statements the obligations of all external organizations supporting its services including the applicable policies and practices.

6.2 Terms and Conditions

OVR-6.2-01: The requirements specified in ETSI EN 319 401 [9], clause 6.2 shall apply.

In addition, the following particular requirements apply:

OVR-6.2-02: To specify the trust service policy being applied, the SCASC terms and conditions shall list or make reference to (e.g. through OIDs), and briefly describe, the supported SCASC policies it conforms to.

OVR-6.2-03: To specify the trust service policy being applied, the SCASC terms and conditions may use the OIDs defined in clause 4.2.2.

OVR-6.2-04: The `main` OID, as defined in clause 4.2.2, shall only be used in relation with an SCASC if the SCASC conforms to the normative requirements in the main part of the present standard (excluding annex B).

OVR-6.2-05: The `eu-advanced-x509` OID, as defined in clause 4.2.2, shall only be used in relation with an SCASC if the SCASC conforms to the normative requirements in the main part of the present standard and the ones in annex B.

OVR-6.2-06: The terms and conditions shall indicate the rights and obligations of the SCASP and the signer.

OVR-6.2-07: The terms and conditions shall describe the options supported by the service. At least:

a) the supported signature formats,

EXAMPLE: CAdES [3], [4], XAdES [5], [6] or PAdES [7],[8].

b) the supported signature parameters,

c) if the to be signed document can be provided only as a hash, and

d) the supported signature creation devices (SCDev) in the user's environment or the supported SSASCs creating the digital signature value for the signer.

OVR-6.2-08: The terms and conditions shall include Service-Level Agreement (SLA) elements for the availability of the service and when applicable, other SLA information such as response times.

OVR-6.2-09: The terms and conditions shall provide a notice that the SLA can be affected by the practices, policies and SLAs of other TSPs, not under the control of the SCASP like the CA issuing the certificate used for the signature or a TSA used for a time-stamp.

OVR-6.2-10: The terms and conditions shall explain how the SCASP processes personal data.

6.3 Information security policy

OVR-6.3-01: The requirements specified in ETSI EN 319 401 [9], clause 6.3 shall apply.

In addition, the following particular requirement apply:

OVR-6.3-02: The security policy should document the security and privacy controls implemented to protect personal data.

NOTE: If the SCASP has access to the to be signed data, then this can contain confidential information as well as personal data.

7 Signature creation application service management and operation

7.1 Internal organization

OVR-7.1-01: The requirements specified in ETSI EN 319 401 [9], clause 7.1 shall apply.

7.2 Human resources

OVR-7.2-01: The requirements specified in ETSI EN 319 401 [9], clause 7.2 shall apply.

7.3 Asset management

OVR-7.3-01: The requirements specified in ETSI EN 319 401 [9], clause 7.3 shall apply.

7.4 Access control

OVR-7.4-01: The requirements specified in ETSI EN 319 401 [9], clause 7.4 shall apply.

7.5 Cryptographic controls

OVR-7.5-01: The requirements specified in ETSI EN 319 401 [9], clause 7.5 shall apply.

7.6 Physical and environmental security

OVR-7.6-01: The requirements specified in ETSI EN 319 401 [9], clause 7.6 shall apply.

In addition the following particular requirement apply:

OVR-7.6-02: The following requirement specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SCA: **GSM 1.4**.

7.7 Operation security

OVR-7.7-01: The requirements specified in ETSI EN 319 401 [9], clause 7.7 shall apply.

In addition, the following particular requirements apply:

OVR-7.7-02: The following requirements specified in ETSI TS 119 101 [1], clause 5.2 should apply to the SCA: **GSM 1.2** and **GSM 1.3**.

OVR-7.7-03: The following requirements specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SCA: **GSM 2.4**.

OVR-7.7-04: The SCASC shall implement all mandatory requirements from ETSI TS 119 101 [1] referenced above regardless of whether the requirement is imposed on the DA or the SCA.

7.8 Network security

OVR-7.8-01: The requirements specified in ETSI EN 319 401 [9], clause 7.8 shall apply.

7.9 Incident management

OVR-7.9-01: The requirements specified in ETSI EN 319 401 [9], clause 7.9 shall apply.

7.10 Collection of evidence

OVR-7.10-01: The requirements specified in ETSI EN 319 401 [9], clause 7.10 shall apply.

In addition the following particular requirements apply:

OVR-7.10-02: Any AdES digital signature creation operation shall be logged, together with identification of the subscriber when this information is known.

OVR-7.10-03: Event logs shall be marked with the time of the event.

OVR-7.10-04: The frequency of processing, the retention period, the protection, the back-up procedures of the collection system, the archiving procedures and the vulnerability assessment of the event logs shall be documented in the SCASC practice statement.

OVR-7.10-05: The implementation of requirements OVR-7.10.1 and OVR-7.10.2 shall take the applicable privacy requirements into account.

OVR-7.10-06: Event logs should include the type of the event, the event success or failure, and an identifier of the person and/or component at the origin for such an event.

7.11 Business continuity management

OVR-7.11-01: The requirements specified in ETSI EN 319 401 [9], clause 7.11 shall apply.

In addition, in order to provide business continuity as specified in the terms and conditions the following particular requirements apply:

OVR-7.11-02: Measures should be implemented to avoid interruptions of the service due to intentional or unintentional behaviour of users or third parties.

OVR-7.11-03: [CONDITIONAL] When adding time-stamps to the signature, the SLA of the SCASP should take the SLA of the corresponding TSA into account.

7.12 Termination and termination plans

OVR-7.12-01: The requirements specified in ETSI EN 319 401 [9], clause 7.12 shall apply.

7.13 Compliance and legal requirements

OVR-7.13-01: The requirements specified in ETSI EN 319 401 [9], clause 7.13 shall apply.

In addition, the following particular requirements apply:

OVR-7.13-02: When personal data is processed by a third party, if needed by the law, an appropriate agreement shall be made with third party processors of personal data in order to ensure that they do comply with the legal requirements, including the implementation of technical, organizational and legal measures to protect the personal data.

NOTE 1: The data to be signed is to be considered as personal data.

OVR-7.13-03: The SCASC shall not store the SD after processing when not necessary.

NOTE 2: If the SCASP works in combination of a preservation service there can be a need to keep such data.

OVR-7.13-04: The SCASP shall have the overall responsibility for meeting the requirements defined in clauses 5 to 8 even when some or all of its functionalities are undertaken by sub-contractors.

8 Signature creation application service component technical requirements

8.1 Interface

ASI-8.1-01: [CONDITONAL] When the SCASC has a machine accessible interface to contact its service, it should use the protocol defined in ETSI TS 119 432 [i.9].

ASI-8.1-02: The connection between the SCASC and the SCDev used for creation of the digital signature value shall be secured.

ASI-8.1-03: [CONDITIONAL] When the SCASC presents the document to the signer, it shall describe in its SCASC practice statement how it guarantees that What You See Is What You Sign (WYSIWYS).

ASI-8-1-04: [CONDITIONAL] When the SCASC presents the document to the signer in an interpreted way, the SCASC practice statement shall clearly state how it interprets specific data.

EXAMPLE: The document to be signed is XML format, and the practice statement states which software is used for the presentation or which rules are followed to present the different XML tags.

ASI-8.1-05: [CONDITIONAL] When the SCASC presents the document to the signer, the SCASC practice statement or the terms and conditions shall state which content types can be correctly presented.

ASI-8.1-06: [CONDITIONAL] When the SCASC presents the document to the signer, the interface shall warn the signer if it cannot accurately present all parts of the SD according to the data content type.

ASI-8.1-07: [CONDITIONAL] When the SCASC provides a graphical user interface to the client the requirements UI 1 and UI 2 from ETSI TS 119 101 [1] should apply.

ASI-8.1-08: [CONDITIONAL] When the SCASC presents the document to the signer, it shall have a workflow where it is clear to the signer that the signer consents to the signing of the document.

ASI-8.1-09: [CONDITIONAL] When the SCASC presents the document to the signer, **SCP 13** and **SCP 47** of ETSI TS 119 101 [1] shall apply.

ASI-8.1-10: [CONDITIONAL] When the SCASC presents the document to the signer, the SCASC should allow to download the document to be signed.

ASI-8.1-11: [CONDITIONAL] When the SCASC presents the document to the signer, the SCASC should log for how long the document was presented to the signer.

ASI-8.1-12: [CONDITIONAL] When the SCASC presents the document to the signer and the document was downloaded, the SCASC should log such an event.

8.2 AdES digital signature creation

OVR-8.2-01: The SCASC shall guarantee the integrity and confidentiality of the received information.

OVR-8.2-02: The cryptographic algorithms used should be selected from algorithms recommended by ETSI TS 119 312 [i.5].

NOTE 1: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations.

OVR-8.2-03: The cryptographic algorithms applied shall be as defined in signature creation policy.

OVR-8.2-04: SCP 14, SCP 31, SCP 37 and **SCP 61** of ETSI TS 119 101 [1] shall apply.

OVR-8.2-05: The SCASC shall inform the signer of the commitment type.

NOTE 2: This information can be given within the signature policy.

OVR-8.2-06: The SCASC should include the signing certificate chain into the signature.

OVR-8.2-07: The signer shall be able to know which signature creation policy will be applied.

OVR-8.2-08: The signer shall be able to know which signature creation policy was applied when creating a specific the signature.

EXAMPLE 1: The information on which signature creation policy will or was applied for a specific signature can be known from the user account of the signer.

EXAMPLE 2: The signature creation policy can be added as a signed attribute to the signature.

EXAMPLE 3: The SCASP has only one signature creation policy in force at each time, and from the time of signature it is clear which version applies.

OVR-8.2-08: The SCASC should provide the signature to the signer.

OVR-8.2-09: [CONDITIONAL] If the SCASC has access to the signed data, it should provide the signed data together with the signature to the signer.

NOTE 3: In case the signature is enveloped in or enveloping the signed data, **OVR-8.2-09** follows directly from **OVR-8.2-08.**

9 Framework for definition of signature creation application service component policy built on the present document

OVR-9-01: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; the policy shall incorporate, or further constrain, all the requirements identified in clauses 5 to 8.

OVR-9-02: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; the policy shall identify any variances it chooses to apply.

OVR-9-03: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; subscribers shall be informed, as part of implementing the terms and conditions, of the ways in which the specific policy adds to or further constrains the requirements of the policy as defined in the present document.

OVR-9-04: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; there shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the policy.

OVR-9-05: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; a risk assessment should be carried out to evaluate business requirements and determine the security requirements to be included in the policy for the stated community and applicability.

OVR-9-06: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; the policy shall be approved and modified in accordance with a defined review process, including responsibilities for maintaining the policy.

OVR-9-07: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; a defined review process shall exist to ensure that the policy is supported by the practices statements.

OVR-9-08: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; the TSP should make available the policies supported by the TSP to its user community.

OVR-9-09: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; revisions to policies supported by the TSP should be made available to subscribers.

OVR-9-10: [CONDITIONAL] When building a SCASC policy built on requirements defined in the present document; a unique object identifier shall be obtained for the policy (e.g. OID or URI).

Annex A (informative): Table of contents for SCASC practice statement

1. Introduction

1.1 Overview

1.1.1 TSP identification

1.1.2 Supported signature creation application service component policy/policies

(*formal OID/URI identification)*

1.2 Signature creation application service component environment

1.2.1 SCASC actors

1.2.3 Service architecture

1.3 Definitions and abbreviations

1.3.1 Definitions

1.3.2 Abbreviations

1.4 Policies and practices

1.4.1 Organization administrating the TSP documentation

1.4.2 Contact person

1.4.3 TSP (public) documentation applicability

This clause describes the set of documents related to the SCASC, their applicability, and position of the present practice statement within the documentation, their distribution points.

At a minimum the following documents exist and need a short description:

- the present practice statement (formal OID/URI identification should be used);
- the terms and conditions;
- the service policy (can be referred)

one or more of the above documents identify the supported signature creation policy/policies (with formal OID/URI identification). The supported signature creation policy/policies are generally detailed in the SCASC service policy/policies.

- risk assessment and Information security policy

NOTE: The description of any business (application) domain or any transactional context can be described in a "signature applicability rules" document. There is no obligation for a TSP to support and publish signature applicability rules.

2. Trust Service management and operation

This clause may be common to all services offered by the TSP – except for CA services where the table of content described by IETF RFC 3647 should be applied.

(Either the same clause is reproduced for each service practice statement, in which case, because every service policy and security requirements add elements specific to the services, such requirements need to be addressed in addition, OR there is a common clause that is referred to from each service practice statement).

2.1 Internal organization

2.1.1 Organization reliability

(This clause identifies the obligations of all external organizations supporting the TSP services including the applicable policies and practices (per ETSI EN 319 401 [9])

2.1.2 Segregation of duties

2.2 Human resources

2.3 Asset management

2.3.1 General requirements

2.3.2 Media handling

2.4 Access control

2.5 Cryptographic controls

2.6 Physical and environmental security

2.7 Operation security

2.8 Network security

2.9 Incident management

2.10 Collection of evidence

2.11 Business continuity management

2.12 TSP termination and termination plans

2.13 Compliance

3. Signature creation application service component technical requirements

3.1 Interfaces

This clause contains requirements, control objectives and controls in connection with clause 8.1. in ETSI TS 119 431-2.

3.2 AdES digital signature creation

This clause contains requirements, control objectives and controls in connection with clause 8.2. in ETSI TS 119 431-2.

Annex B (normative): EU specific requirements related to Regulation (EU) No 910/2014 for creation of advanced electronic signatures and seals based on X.509 certificates

NOTE: This clause aims at providing best practices for the creation of advanced electronic signatures/seals based on X.509 certificates.

OVR-B.1-01: [CONDITONAL] Where the SCASC is used to create an advanced electronic signature, the signing certificate shall identify the signatory.

OVR-B.1-02: [CONDITONAL] Where the SCASC is used to create an advanced electronic seal, the signing certificate shall identify the creator of the seal.

OVR-B.1-03: The signing certificate shall be contained in the created AdES signature.

Annex C (informative): Mapping to advance electronic signatures or seals as by Regulation (EU) No 910/2014

Table C.1 maps the requirements from the present document with the requirements on advanced electronic signatures or seals as specified directly by Regulation (EU) No 910/2014 [i.1] (Tables 1 and 2) or indirectly via requirements on valid QES as specified by Regulation (EU) No 910/2014 [i.1] (Table 3).

Table C.1: Mapping of the requirements in the present document to requirements for advanced electronic signatures as defined by Regulation (EU) No 910/2014

Regulation (EU) No 910/2014	Applicable requirements
Article 26 **Requirements for advanced electronic signatures** *"An advanced electronic signature shall meet the following requirements:*	
(a) it is uniquely linked to the signatory;	**OVR-B.1-01** **OVR-8.2-04** referencing from ETSI TS 119 101 [1] **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*."
(b) it is capable of identifying the signatory;	**OVR-B.1-03**
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and	The sole control is out of scope of the present document. If a SSASC is used, this is covered in ETSI TS 119 431-1 [i.8]. See note.
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable."	**OVR-8.2-02** The cryptographic algorithms used should be selected from algorithms recommended by ETSI TS 119 312 [i.5].
NOTE: The SSASC can limit the list of supported SCDev in its terms and conditions (OVR-6.2-05).	

Table C.2: Mapping of the requirements in the present document to requirements for advanced electronic seals as defined by Regulation (EU) No 910/2014

Regulation (EU) No 910/2014	Applicable requirements
Article 36 **Requirements for advanced electronic seals** *"An advanced electronic seal shall meet the following requirements:*	
(a) it is uniquely linked to the creator of the seal;	**OVR-B.1-02** OVR-8.2-04 referencing from ETSI TS 119 101 [1] **SCP 37**
(b) it is capable of identifying the creator of the seal;	**OVR-B.1-03**
(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and	The sole control is out of scope of the present document. If a SSASC is used, this is covered in ETSI TS 119431-1 [i.8]. See note.
(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable."	**OVR-8.2-04** referencing from ETSI TS 119 101 [1] **SCP 14**
NOTE: The SSASC can limit the list of supported SCDev in its terms and conditions (OVR-6.2-05).	

Table C.3: Mapping of the requirements in the present document to requirements that have to be fulfilled for a valid advanced electronic signature/seal as defined by Regulation (EU) No 910/2014

Regulation (EU) No 910/2014	Applicable requirements
Article 32.1 **Requirements for the validation of qualified electronic signatures** *"1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:*	
(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;	Not applicable, specific to the qualified case
(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;	Not applicable, specific to the qualified case
(c) the signature validation data corresponds to the data provided to the relying party;	Not applicable, this is the responsibility of the CA and the SSASC
(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;	Not applicable, this is the responsibility of the CA
(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;	Not applicable, this is the responsibility of the CA
(f) the electronic signature was created by a qualified electronic signature creation device;	Not applicable, specific to the qualified case
(g) the integrity of the signed data has not been compromised;	**OVR-8.2-02**
(h) the requirements provided for in Article 26 were met at the time of signing."	See table C.1

History

Document history		
V1.1.1	December 2018	Publication