ETSI TS 119 431-1 V1.1.1 (2018-12)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for trust service providers;
Part 1: TSP service components operating a remote QSCD / SCDev

Reference
DTS/ESI-0019431-1

Keywords
e-commerce, electronic signature, remote,
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

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 1 of a multi-part deliverable covering policy and security requirements for Trust Service Providers providing remote signature, 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 operating a digital signature creation device, including a QSCD (Qualified Signature/Seal Creation Device) as defined in Regulation (EU) No 910/2014 [i.1] to create a digital signature value on behalf of a remote signer.

These requirements are based on the general policy requirements specified in ETSI EN 319 401 [1] and take into account related requirements for certificate issuance in ETSI EN 319 411-1 [2].

The requirements of the present document are aligned with the requirements specified in CEN EN 419 241-1 [3].

Introduction

When digital signatures are created in an entirely user-managed environment, it is assumed that the signature creation data is under the control of the signer, who is physically in possession of the signature creation device.

For remote digital signature creation, the signature creation data is maintained and managed by a third party on behalf of the signer. To guarantee that the signature creation environment is reliable and that the signature creation data is used under the control of the signer, the provider of the remote digital signature service has to apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels.

1 Scope

The present document specifies generally applicable policy and security requirements for Trust Service Providers (TSP) implementing a service component operating a remote signature creation device (SCDev). Specific requirements apply when the device is a QSCD as defined in Regulation (EU) No 910/2014 [i.1].

The service component consists of a signing application and a QSCD / SCDev. The term used in the present document is server signing application service component (SSASC).

The policy and security requirements are defined in terms of requirements for creation, maintenance, life-cycle management and use of signing keys used to create digital signatures.

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

The present document is aimed to be used by independent bodies as the basis for a conformity assessment that a TSP can be trusted for operating a remote QSCD / SCDev.

The present document supports European and other regulatory frameworks.

NOTE 1: Specifically, but not exclusively, the present document is aimed at qualified and non-qualified trust service providers, providing the creation of digital signatures supporting electronic signatures and electronic seals (both advanced and qualified) in accordance with the requirements of Regulation (EU) No 910/2014 [i.1]. Annex A contains requirements that are specific for an SSASC in the context of Regulation (EU) No 910/2014 [i.1].

The present document does neither specify how fulfilment of the requirements can be assessed by an independent conformity assessment body, nor requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE 2: See ETSI EN 319 403 [i.3] for guidance on assessment of a TSP's processes and services.

NOTE 3: The present document references ETSI EN 319 401 [1] for general policy requirements common to all TSP services covered by ETSI standards.

The present document does not specify protocols used to access the SSASC.

NOTE 4: Protocols for remote digital signature creation are defined in ETSI TS 119 432 [i.4].

The present document identifies specific controls needed to address risks associated with services operating remote QSCD / SCDev.

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

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

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

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

[i.4] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

[i.5] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.6] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.7] ISO/IEC 18014-2: "Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens".

[i.8] CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing".

[i.9] CEN 419 221-5: " Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services".

[i.10] ETSI 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

3 Definition of terms, abbreviations and notations

3.1 Terms

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

NOTE: Where a definition is copied from a referenced document this is indicated by inclusion of the reference identifier number at the end of the definition.

authentication: provision of assurance in the claimed identity of an entity

NOTE: As defined in ISO/IEC 18014-2 [i.7].

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

electronic identification (eID): process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person

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

electronic identification means: material and/or immaterial unit containing person identification data and which is used for authentication for an online service

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

electronic identification means reference: data used in the SSASC as a reference to an electronic identification means in order to authenticate the signer

EXAMPLE: When the eID means uses asymmetric keys, the public key can be the reference.

When a signed assertion is generated after a successful authentication of the signer, the assertion signer id and the user id can be the reference.

When the eID means uses a secret key (e.g. one time password generator) the secret key can be the reference.

person identification data: set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established

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

qualified electronic signature/seal creation device (QSCD): as specified in Regulation (EU) No 910/2014 [i.1]

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 service component (SSASC): TSP service component employing a server signing application to create a digital signature value on behalf of a signer

server signing application service provider (SSASP): TSP operating a server signing application service component

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

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

trust service provider (TSP): entity which provides one or more trust services

3.2 Abbreviations

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

eID	electronic IDentification
EUSCP	EU SSASC Policy
LSCP	Lightweight SSASC Policy
NCP	Normalized Certificate Policy
NSCP	Normalized SSASC Policy
OID	Object IDentifier
QSCD	Qualified electronic Signature/Seal Creation Device
SCDev	Signature Creation Device
SCP	SSASC Policy
SSASC	Server Signing Application Service Component
SSASP	Server Signing Application Service Provider
TSP	Trust Service Provider

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any SSASC policies. 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]";

c) requirements that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]";

d) requirements applicable to the services offered under the applicable SSASC policy. Such requirements are indicated by clauses marked by the applicable SSASC policy as follows:

"[LSCP]", "[NSCP]" and "[EUSCP]".

The requirements in the present document are identified as follows:

<3 letters service component> - < the clause number> - <2 digit number - incremental>

The SSASC service sub-components are:

- **OVR:** General requirement (requirement applicable to more than 1 service component)
- **GEN:** Signing Key Generation Service
- **LNK:** Certificate/eID means Linking Service
- **SIG:** Signature Activation Service
- **DEL:** Signing Key Deletion Service
- **EID:** eID Means Provision (optional)

The management of the requirement identifiers throughout 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 a new requirement.
- 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 broadly in line with ETSI EN 319 411-1 [2] to assist TSPs in applying these requirements to their own policy and practice statement documentation.

The present document incorporates CEN EN 419 241-1 [3] requirements by reference. CEN EN 419 241-1 [3] defines levels of assurance for sole control. The term "sole control" does not mean that the requirements are only applicable to electronic signatures as defined in Regulation (EU) No 910/2014 [i.1]. The requirements may be applied mutatis mutandis to electronic seals. In other words, the reader may replace the term "sole control" with "control" as explained in CEN EN 419 241-1 [3] clause 5.3.

NOTE 1: Any applicable and referenced requirements on the TW4S is a requirement on the SSASC.

The present document incorporates ETSI EN 319 401 [1] requirements by reference and adds requirements relevant for a SSASP. See ETSI EN 319 401 [1], clause 4 and IETF RFC 3647 [i.5], clauses 3.1 and 3.4 for guidance.

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objectives will be met.

NOTE 2: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a TSP can employ in operating signing devices. In some cases, reference is made to other more general standards which can be used as a source of more detailed control requirements. Due to these factors the specificity of the requirements given under a given topic can vary.

The present document includes the provision of services for key generation, certificate linking, eID means linking, signature activation, key deletion and device provisioning (see clause 4.4).

4.2 Relationships between the TSP issuing certificates and the SSASC

An SSASC may be part of the services provided by a TSP issuing certificates, part of the services of another type of TSP, or be provided by a TSP supporting only the SSASC. In all cases this TSP is identified as SSASP.

NOTE: When the SSASP is the TSP issuing certificates then some requirements of the present document can be met by a service component of the CA.

4.3 SSASC applicable documentation

4.3.1 SSASC practice statement

The **server signing application service provider (SSASP)** develops, implements, enforces, and updates a **SSASC practice statement**, which is a trust service practice statement as defined in ETSI EN 319 401 [1], instantiated for a SSASC. See clause 6.1.

The SSASC practice statement describes ***how*** the SSASP operates its service and is owned by the SSASP. The SSASC 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 SSASC practice statement as requested in the present document, however the present document places no restriction on the form of the SSASC practice statement; it can be included in a general TSP practice statement document that covers other services delivered by that TSP or be a standalone document.

The present document provides requirements identified as necessary for SSASC policies defined in clause 4.3.2, to be endorsed by a SSASP and reflected in its **practice statement**.

4.3.2 SSASC policy

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

The present document defines three SCPs:

1) A Lightweight SSASC Policy (LSCP) offering a quality of service less onerous than the NSCP (requiring less demanding policy requirements) for use where a risk assessment does not justify the additional burden of meeting all requirements of the NSCP (e.g. use of a signature activation module).

2) A Normalized SSASC Policy (NSCP) which meets general recognized best practice for TSPs operating a remote SCDev used in support of any type of transaction.

3) An EU SSASC Policy (EUSCP) which offers the same quality as that offered by the NSCP but with specific requirements from the Regulation (EU) No 910/2014 [i.1] related to QSCD management.

NOTE: EUSCP specific requirements are defined in Annex A.

A SCP is not necessarily part of the SSASP's documentation (as per ETSI EN 319 401 [1] a practice statement and general terms and conditions are sufficient); e.g. a SCP can be shared by a community and not owned by the SSASP. Also, the present document does not put constraints on the form of the SCP; a SCP can be a stand-alone document or be provided as part of the practice statement and / or the general terms and conditions.

4.3.3 Terms and conditions

In addition to, or as part of, the SCP and the SSASC practice statement, a TSP issues terms and conditions. Terms and conditions can cover a broad range of commercial terms or technical terms. The terms and conditions are specific to a SSASP. The recipients of the terms and conditions are subscribers and 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.

4.4 SSASC sub-component services

NOTE 1: The present document does not mandate any sub division of the services of a TSP. Requirements are stated in subsequent clauses.

The SSASC services are broken down in the present document into the following sub-component services for the purposes of classifying requirements:

- **Signing key generation service:** generates signing keys in the remote device. The proof of possession of generated signing keys are passed to the registration service of the TSP issuing the associated certificate.
- **Certificate linking service:** links the certificates generated by the certificate generation service of a TSP with the corresponding signing keys.
- **eID means linking service**: links eID means references with the corresponding signing keys in order to provide sole control. The service can be used to support requirement REG-6.3.1-01 in ETSI EN 319 411-1 [2] for a TSP issuing certificates.

EXAMPLE 1: By providing an assertion of the authentication of the signer that is linked to the private key.

- **Signature activation service:** verifies the signature activation data and activates the corresponding signing key in order to create a digital signature.
- **Signing key deletion service:** destroys signing keys in a way that ensures that the signing keys cannot be used anymore.
- **eID means provision service (optional):** prepares and provides or makes eID means available to the signers.

EXAMPLE 2: a service which generates the authentication key and distributes the key to the subject of the certificate (this includes "soft" keys i.e. keys protected by software environment);

a service which prepares the authentication device and enabling codes, and distributes them to the subject of the certificate (this includes keys protected by hardware environment).

This subdivision of services is only for the purposes of clarification of policy requirements and places no restrictions on any subdivision of an implementation of the TSP's services.

Figure 1 illustrates the interrelationships between the service sub-components of the present document and relations with external component services of the TSP issuing the signing certificates.

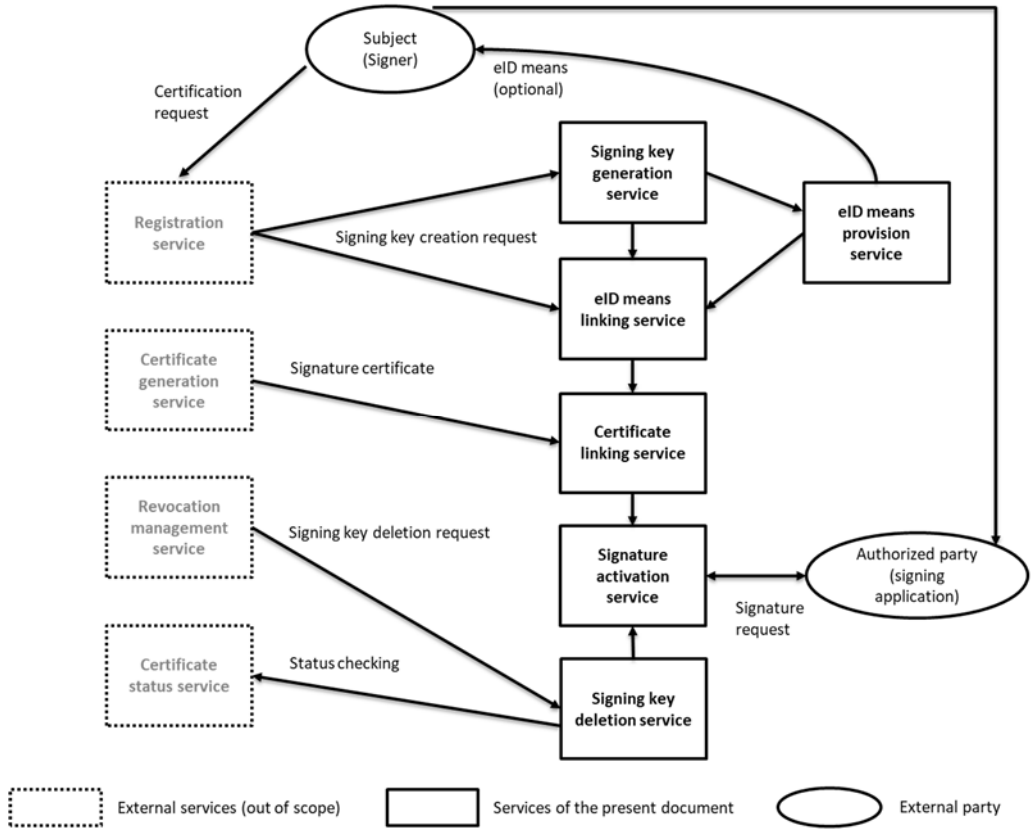

Figure 1: Illustration of subdivision of SSASC sub-components

Figure 2 illustrates the interrelationships between the services of the present document and relations with an authentication process delegated to an external party.

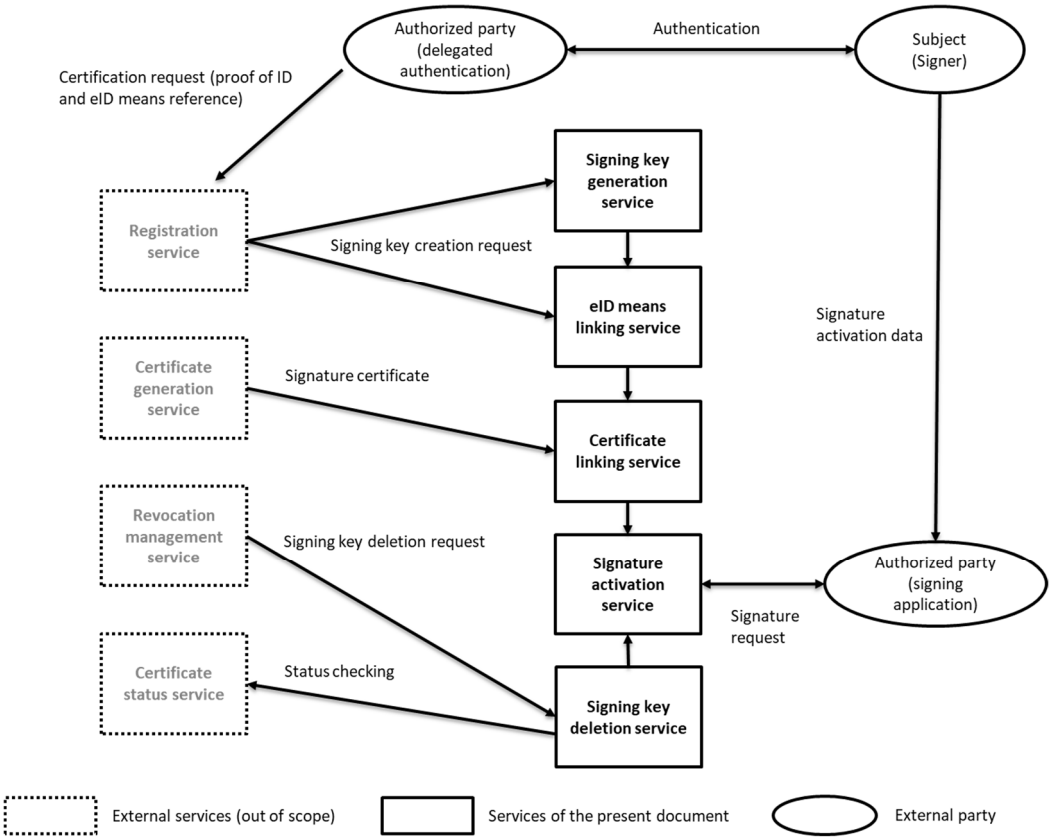

Figure 2: Illustration of subdivision of SSASC sub-components with delegated authentication

NOTE 2: Figures 1 and 2 are for illustrative purposes and do not show a processing flow. Clause 6 specifies the specific requirements for each of the services.

5 General provisions on practice statement and policies

5.1 Practice statement requirements

OVR-5.1-01: The general requirements specified in ETSI EN 319 401 [1], clause 6.1 shall apply.

In addition, the following particular requirements apply:

NOTE 1: A TSP can document practices relating to specific SSASC policy requirements separate from the main practice statement document.

OVR-5.1-02: The TSP's practice statement shall include the signature algorithms and parameters applied, the algorithms applied for key pair generation and any other algorithms and parameters that are critical to the security of the SSASC operation.

OVR-5.1-03: The TSP shall publicly disclose its practice statement through an online means that is available on a 24x7 basis.

NOTE 2: The TSP is not obliged to disclose any aspects containing sensitive information.

5.2 SCP name and identification

SSASPs following the present document can claim conformance to the present document via the following specific trust service policy OID:

a) LSCP: Lightweight SSASC Policy

```
itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops  (1)
policy-identifiers(1) lightweight (1)
```

b) NSCP: Normalized SSASC Policy

```
itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops(1)
policy-identifiers(1) normalized (2)
```

NOTE: Annex A defines an additional SSASC policy with specific requirements related to Regulation (EU) No 910/2014 [i.1].

OVR-5.2-01: If any changes are made to a SCP as described in clause 4.3.2 which affects the applicability then the policy identifier should be changed.

5.3 Participants

5.3.1 SSASP

OVR-5.3.1-01: The SSASP may make use of other parties to provide parts of the service, however, the SSASP always maintains overall responsibility and shall ensure that the policy requirements identified in the present document are met.

NOTE: If the external party uses an eID means issued under: a notified scheme that is included in the list published by the Commission pursuant to Article 9 of [i.1], there is no need to demonstrate the conformance to the required level, conformance to the regulatory requirements can be assumed.

5.3.2 Subscriber and signer

In the framework of the present policies, the signer associated to the signing key can be:

- a natural person;
- a natural person identified in association with a legal person;
- a legal person (that can be an organization or a unit or a department identified in association with an organization); or
- a device or system operated by or on behalf of a natural or legal person.

NOTE: This present document does not place any specific restrictions on the legal representation implied by an electronic signature or seal created using the present document.

The relationship between the signer and the subscriber is equivalent to the relationship between subject and subscriber as described in ETSI EN 319 411-1 [2] clause 5.4.2.

6 Trust Service Providers practice

6.1 Publication and repository responsibilities

OVR-6.1-01: The TSP shall make available to subscribers and relying parties the applicable SCPs, practice statements and terms and conditions regarding the use of signing keys.

OVR-6.1-02: The applicable terms and conditions shall be readily identifiable for a given signing key or for the associated certificate.

OVR-6.1-03: The information identified in **OVR-6.1-01** and **OVR-6.1-02** above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the SSASC practice statement.

OVR-6.1-04: The information identified in **OVR-6.1-01** above should be publicly and internationally available.

6.2 Signing key initialization

6.2.1 Signing key generation

GEN-6.2.1-01 [LSCP]: Clause SRG_KM.1.1 of CEN EN 419 241-1 [3], specifying signing keys environment shall apply.

GEN-6.2.1-02 [NSCP]: Clause SRA_SKM.1.1 of CEN EN 419 241-1 [3], specifying signing keys environment shall apply.

GEN-6.2.1-03: Clause SRG_KM.1.2 of CEN EN 419 241-1 [3], specifying cryptographic algorithms and key lengths, shall apply.

GEN-6.2.1-04: Clause SRG_KM.1.3 of CEN EN 419 241-1 [3], specifying key protection shall apply.

GEN-6.2.1-05: Clause SRG_KM.1.4 of CEN EN 419 241-1 [3], specifying device initialization shall apply.

GEN-6.2.1-06: Clause SRC_SKS.1.1 of CEN EN 419 241-1 [3], specifying algorithm parameters shall apply.

GEN-6.2.1-07: Clause SRC_SKS.1.3 of CEN EN 419 241-1 [3], specifying time of generation shall apply.

GEN-6.2.1-08 [CONDITIONAL]: If the SSASC and the certificate generation service component are managed separately, then the SSASC shall support the requirement defined in clause REG-6.3.1-01 of ETSI EN 319 411-1 [2].

EXAMPLE: By providing an assertion of the authentication of the signer that is linked to the private key.

6.2.2 eID means linking

LNK-6.2.2-01: Clause SRC_SA.1.1 of CEN EN 419 241-1 [3], specifying enrolment shall apply.

LNK-6.2.2-02 [NSCP] [CONDITIONAL]: If the signer is a natural person, clause SRA_SAP.1.1 of CEN EN 419 241-1 [3], specifying enrolment shall apply.

LNK-6.2.2-03: The SSASP shall link signing keys with the appropriate signer's eID means reference.

LNK-6.2.2-04: The SSASP may generate eID means reference and provide the corresponding eID means to the signer (see clause 6.2.4).

LNK-6.2.2-05: The SSASP shall ensure that the person identification data linked to the eID means reference is the same as the one linked to the subject of the associated certificate.

NOTE 1: When the eID means reference is provided by the TSP issuing certificates registration service, the conformance to this requirement can be assumed.

LNK-6.2.2-06: The signer's eID means reference may be provided by an authorized (external) party.

LNK-6.2.2-07 [LSCP] [CONDITIONAL]: If all or part of the authentication process is delegated to an external party the SSASP shall ensure the external party meets the requirements specified in LNK-6.2.2-01.

NOTE 2: If the external party uses an eID means issued under a notified scheme that is included in the list published by the Commission pursuant to Article 9 of Regulation (EU) No 910/2014 [i.1], there is no need to demonstrate the conformance to the required level, conformance to the regulatory requirements can be assumed.

LNK-6.2.2-08 [NSCP] [CONDITIONAL]: If all or part of the authentication process is delegated to an external party the SSASP shall ensure that the external party meets the requirements specified in LNK-6.2.2-02 and LNK-6.2.2-03.

LNK-6.2.2-09 [NSCP] [CONDITIONAL]: If all or part of the authentication process is delegated to an external party the SSASP shall ensure that:

- the external party fulfils all the relevant requirements of the present document and the requirements for registration according to the applicable regulatory requirements, or

NOTE 3: In the context of the European Union, the applicable regulatory requirements are defined in [i.1].

- the authentication process delegated to the external party uses an eID means issued under a notified scheme in accordance with the applicable regulatory requirements.

NOTE 4: In the context of the European Union, the list of electronic identification means, issued under notified schemes, is published by the European Commission pursuant to Article 9 of Regulation (EU) No 910/2014 [i.1].

LNK-6.2.2-10: The SSASP shall protect the integrity of links between signer's signing key and its eID means reference.

6.2.3 Certificate linking

LNK-6.2.3-01: Clause SRC_SKS.1.2 of CEN EN 419 241-1 [3], specifying certificate linking shall apply to the SSASC.

LNK-6.2.3-02: Clause SRC_SKS.1.4 of CEN EN 419 241-1 [3], specifying certificate linking shall apply to the SSASC.

LNK-6.2.3-03: Clause SRC_SKS.1.5 of CEN EN 419 241-1 [3], specifying links protection shall apply to the SSASC.

6.2.4 eID means provision

EID-6.2.4-01 [CONDITIONAL]: If the SSASP provides the signer's eID means, the eID means shall be securely passed to the signer.

EID-6.2.4-02 [CONDITIONAL]: If the SSASP personalizes the signer's eID means with an associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the signer's eID means.

6.3 Signing key life-cycle operational requirements

6.3.1 Signature activation

SIG-6.3.1-01: Clause SRC_SA.1.2 of CEN EN 419 241-1 [3], specifying authentication shall apply.

SIG-6.3.1-02: Clause SRC_SA.1.3 of CEN EN 419 241-1 [3], specifying protocol security shall apply.

SIG-6.3.1-03: Clause SRC_SA.1.4 of CEN EN 419 241-1 [3], specifying access control shall apply.

SIG-6.3.1-04: Clause SRC_SA.1.5 of CEN EN 419 241-1 [3], specifying signing key control shall apply.

SIG-6.3.1-05 [NSCP]: Clause SRA_SKM.2.1 of CEN EN 419 241-1 [3], specifying signing key activation shall apply.

SIG-6.3.1-06 [NSCP]: Clause SRA_SAP.1.2 of CEN EN 419 241-1 [3], specifying protocol security shall apply.

SIG-6.3.1-07 [NSCP]: Clause SRA_SKM.2.5 of CEN EN 419 241-1 [3], specifying signing key control shall apply.

SIG-6.3.1-08: The SSASP should ensure that the public key certificate is valid before using the corresponding signing key.

NOTE: valid = not expired not revoked not suspended, can be met by applying DEL-6.3.2-01 if suspension is not used.

SIG-6.3.1-09: Signing keys shall be usable in only those cases for which the signer's consent has been obtained.

SIG-6.3.1-10: Clause SRC_DSC.1.1 of CEN EN 419 241-1 [3], specifying signature creation's algorithm parameters shall apply.

6.3.2 Signing key deletion

DEL-6.3.2-01: Clause SRG_KM.7.1 of CEN EN 419 241-1 [3] shall apply. If the public key certificate is revoked, the corresponding signing key shall be destroyed.

DEL-6.3.2-02: The SSASP shall destroy a signing key when requested by the signer.

DEL-6.3.2-03: Clause SRG_KM.7.2 of CEN EN 419 241-1 [3], specifying session management shall apply.

DEL-6.3.2-04: Clause SRG_KM.7.3 of CEN EN 419 241-1 [3], specifying key backup deletion shall apply.

6.3.3 Signing key backup and recovery

GEN-6.3.3-01: Clause SRG_KM.2.1 of CEN EN 419 241-1 [3], specifying key backup shall apply.

GEN-6.3.3-02: Clause SRG_KM.2.2 of CEN EN 419 241-1 [3], specifying backup protection shall apply.

GEN-6.3.3-03: Clause SRG_KM.2.3 of CEN EN 419 241-1 [3], specifying backup controls shall apply.

GEN-6.3.3-04: The number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

6.4 Facility, management, and operational controls

6.4.1 General

OVR-6.4.1-01: The requirements identified in ETSI EN 319 401 [1], clauses 5, 6.3 and 7.3, shall apply.

6.4.2 Physical security controls

OVR-6.4.2-01: The requirements identified in ETSI EN 319 401 [1], clause 7.6 shall apply.

In addition, the following particular requirements apply:

OVR-6.4.2-02: The requirements identified in ETSI EN 319 411-1 [2], clause OVR-6.4.2-02 to OVR-6.4.2-11 shall apply mutatis mutandis to signing key generation and activation management services.

6.4.3 Procedural controls

OVR-6.4.3-01: The requirements REQ-7.4-04 to REQ-7.4-09 in ETSI EN 319 401 [1] shall apply.

6.4.4 Personnel controls

OVR-6.4.4-01: The requirements identified in ETSI EN 319 401 [1], clause 7.2 shall apply.

6.4.5 Audit logging procedures

OVR-6.4.5-01: The requirements identified in ETSI EN 319 401 [1], clause 7.10 shall apply.

OVR-6.4.5-02: All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and SSASC system access attempts.

OVR-6.4.5-03: Clause SRG_AA.1 of CEN EN 419 241-1 [3], specifying audit data generation shall apply.

OVR-6.4.5-04: Clause SRG_AA.2 of CEN EN 419 241-1 [3], specifying audit data availability shall apply.

OVR-6.4.5-05: Clause SRG_AA.3 of CEN EN 419 241-1 [3], specifying audit data parameters shall apply.

OVR-6.4.5-06: Clause SRG_AA.7 of CEN EN 419 241-1 [3], specifying audit data integrity shall apply.

OVR-6.4.5-07: Clause SRG_AA.8 of CEN EN 419 241-1 [3], specifying audit data timing shall apply.

6.4.6 Records archival

OVR-6.4.6-01: The SSASP shall retain the audit data records for at least seven years after any certificate based on these records ceases to be valid and within the constraint of applicable legislation

6.4.7 Key changeover

No policy requirement.

6.4.8 Compromise and disaster recovery

OVR-6.4.8-01: The requirements identified in ETSI EN 319 401 [1], clauses 7.9 and 7.11 shall apply.

6.4.9 SSASP service termination

OVR-6.4.9-01: The requirements identified in ETSI EN 319 401 [1] , clause 7.12 shall apply.

6.5 Technical security controls

6.5.1 Systems and security management

OVR-6.5.1-01: The requirements identified in CEN EN 419 241-1 [3], clause SRG_M.1 shall apply.

6.5.2 Systems and operations

OVR-6.5.2-01: The requirements identified in CEN EN 419 241-1 [3], clause SRG_SO.1 shall apply.

OVR-6.5.2-02: The requirements identified in CEN EN 419 241-1 [3], clause SRG_SO.2 shall apply.

6.5.3 Computer security controls

OVR-6.5.3-01: The requirements REQ-7.4-01, REQ-7.4-02, REQ-7.4-03 and REQ-7.4-10 in ETSI EN 319 401 [1] shall apply.

NOTE: Requirements for the trustworthy systems can be ensured using, for example, systems conforming to CEN EN 419 241-1 [3] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [i.6].

OVR-6.5.3-02: Clause SRG_AA.6.1 of CEN EN 419 241-1 [3], regarding system monitoring shall apply.

6.5.4 Life cycle security controls

OVR-6.5.4-01: The requirements identified in ETSI EN 319 401 [1], clause 7.7 shall apply for all service components.

6.5.5 Network security controls

OVR-6.5.5-01: The requirements identified in ETSI EN 319 401 [1], clause 7.8 shall apply.

6.6 Compliance audit and other assessment

NOTE: See ETSI EN 319 403 [i.3].

6.7 Other business and legal matters

6.7.1 Fees

These policy requirements are not meant to imply any restrictions on charging for TSP's services.

6.7.2 Financial responsibility

OVR-6.7.2-01: The requirement REQ-7.1.1-04 identified in ETSI EN 319 401 [1] shall apply.

6.7.3 Confidentiality of business information

No policy requirement.

6.7.4 Privacy of personal information

OVR-6.7.4-01: The requirement REQ 7.13-05 identified in ETSI EN 319 401 [1] shall apply.

6.7.5 Intellectual property rights

No policy requirement.

6.7.6 Representations and warranties

OVR-6.7.6-01: The requirements REQ-6.3-05 and REQ-6.3-06 identified in ETSI EN 319 401 [1] shall apply.

NOTE: The SSASP has the responsibility for conformance with the procedures prescribed in this policy, even when the SSASP's functionality is undertaken by outsourcers.

6.7.7 Disclaimers of warranties

See clause 6.7.6.

6.7.8 Limitations of liability

Limitations on liability are covered in the terms and conditions as per clause 6.8.4.

6.7.9 Indemnities

No policy requirement.

6.7.10 Term and termination

No policy requirement.

6.7.11 Individual notices and communications with participants

No policy requirement.

6.7.12 Amendments

No policy requirement.

6.7.13 Dispute resolution procedures

OVR-6.7.13-01: The item (h) of requirement REQ-6.2-02 identified in ETSI EN 319 401 [1] and the requirement REQ-7.1.1-06 identified in ETSI EN 319 401 [1] shall apply.

6.7.14 Governing law

Not in the scope of the present document.

6.7.15 Compliance with applicable law

OVR-6.7.15-01: The requirements REQ-7.13-01 and REQ-7.13-02 identified in ETSI EN 319 401 [1] shall apply.

6.7.16 Miscellaneous provisions

No policy requirement.

6.8 Other provisions

6.8.1 Organizational

OVR-6.8.1-01: The requirements identified in ETSI EN 319 401 [1], clause 7.1 shall apply.

6.8.2 Additional testing

No policy requirement.

6.8.3 Disabilities

OVR-6.8.3-01: The requirements REQ-7.13-03 and REQ-7.13-04 identified in ETSI EN 319 401 [1] shall apply.

6.8.4 Terms and conditions

OVR-6.8.4-01: The requirements identified in ETSI EN 319 401 [1], clause 6.2 shall apply.

7 Framework for definition of server signing application service component policy built on the present document

OVR-7-01 [CONDITIONAL]: When building a SCP from requirements defined in the present document, the policy shall incorporate, or further constrain, all the requirements identified in clauses 5 to 6.

OVR-7-02 [CONDITIONAL]: When building a SCP from requirements defined in the present document, the policy shall identify any variances it chooses to apply.

OVR-7-03 [CONDITIONAL]: When building a SCP from 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-7-04 [CONDITIONAL]: When building a SCP from 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-7-05 [CONDITIONAL]: When building a SCP from 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-7-06 [CONDITIONAL]: When building a SCP from requirements defined in the present document, the policy should be approved and modified in accordance with a defined review process, including responsibilities for maintaining the policy.

OVR-7-07 [CONDITIONAL]: When building a SCP from requirements defined in the present document, a defined review process should exist to ensure that the policy is supported by the practices statements.

OVR-7-08 [CONDITIONAL]: When building a SCP from requirements defined in the present document, the TSP should make available the policies supported by the TSP to its user community.

OVR-7-09 [CONDITIONAL]: When building a SCP from requirements defined in the present document, revisions to policies supported by the TSP should be made available to subscribers.

OVR-7-10 [CONDITIONAL]: When building a SCP from requirements defined in the present document, a unique object identifier shall be obtained for the policy (e.g. OID or URI).

Annex A (normative): Specific requirements related to Regulation (EU) No 910/2014

A.1 SSASP as a Qualified TSP

The present annex specifies generally applicable policy and security requirements for a Qualified TSP implementing a service component operating a remote QSCD.

OVR-A.1-01 [EUSCP]: The SSASP shall be a Qualified TSP as defined in [i.1].

NOTE 1: The current general interpretation of Regulation (EU) No 910/2014 [i.1] is that the SSASP cannot be qualified for operating the server signing application service component (SSASC) only. The SSASP managing a QSCD, is required to be used as part of a qualified trust service as defined in Regulation (EU) No 910/2014 [i.1]

NOTE 2: See Regulation (EU) No 910/2014 [i.1] Article 3 (16) for trust service definitions.

A.2 Policy name and identification

SSASPs following the present document can claim conformance to the present document via the following specific trust service policy OID:

a) EUSCP: EU SSASC Policy

```
itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops  (1)
policy-identifiers(1) eu-remote-qscd (3)
```

A.3 General requirements

OVR-A.3-01 [EUSCP]: All requirements specified for [NSCP] shall apply.

OVR-A.3-02 [EUSCP]: The TSP's practice statement shall include the reference to the certification that the QSCD employed against the requirements of Regulation (EU) No 910/2014 [i.1], annex II.

A.4 Signing key generation

GEN-A.4-01 [EUSCP]: Signer's signing key shall be generated in a QSCD.

GEN-A.4-02 [EUSCP]: The QSCD shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.

A.5 Signature activation

SIG-A.5-01 [EUSCP]: Signer's signing key shall be used in a QSCD.

SIG-A.5-02 [EUSCP] The QSCD shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.

SIG-A.5-03 [EUSCP]: Clause SRA_SAP.1.3 of CEN EN 419 241-1 [3], specifying cryptographic strength shall apply.

SIG-A.5-04 [EUSCP]: Clause SRA_SAP.1.4 of CEN EN 419 241-1 [3], specifying threats mitigation shall apply.

SIG-A.5-05 [EUSCP]: Clause SRA_SAP.1.5 of CEN EN 419 241-1 [3], specifying environment protection shall apply.

SIG-A.5-06 [EUSCP]: Clause SRA_SAP.1.6 of CEN EN 419 241-1 [3], specifying protection against tampering shall apply.

SIG-A.5-07 [EUSCP]: Clause SRA_SAP.1.7 of CEN EN 419 241-1 [3], specifying protection against attacker shall apply.

A.6 Signature activation data management

SIG-A.6-01 [EUSCP]: Clause SRA_SAP.2.1 of CEN EN 419 241-1 [3], specifying signature activation data format shall apply.

SIG-A.6-02 [EUSCP]: Clause SRA_SAP.2.2 of CEN EN 419 241-1 [3], specifying signature activation data collection and generation shall apply.

SIG-A.6-03 [EUSCP]: Clause SRA_SAP.2.3 of CEN EN 419 241-1 [3], specifying signature activation data parameters shall apply.

SIG-A.6-04 [EUSCP]: Clause SRA_SAP.2.4 of CEN EN 419 241-1 [3], specifying signature activation data usage shall apply.

SIG-A.6-05 [EUSCP]: Clause SRA_SAP.2.5 of CEN EN 419 241-1 [3], specifying signature activation data destination, shall apply.

SIG-A.6-06 [EUSCP] [CONDITIONAL]: If the signer is a natural person, clause SRA_SAP.2.6 of CEN EN 419 241-1 [3], specifying signature activation data collection and protection shall apply.

SIG-A.6-07 [EUSCP] [CONDITIONAL]: If the signer is a natural person, clause SRA_SAP.2.7 of CEN EN 419 241-1 [3], specifying signature activation data submission under sole control shall apply.

SIG-A.6-08 [EUSCP]: Clause SRA_SAP.2.8 of CEN EN 419 241-1 [3], specifying signature activation data protection after activation shall apply.

Annex B (informative): Regulation and EU SSASC policy mapping

Table B.1 identifies how the security controls objectives and other parts of the EU SSASC policy (EUSCP) defined in the present document address the requirements of TSP implementing a service component operating a remote QSCD as defined in recital 52 and annexes of Regulation (EU) No 910/2014 [i.1] in the context of electronic signature. Table B.2 is the same but in the context of electronic seal.

Annex B should not be taken as definitive statement of conformance to the Regulation (EU) No 910/2014 [i.1]. There are requirements in the Regulation (EU) No 910/2014 [i.1] which are not technical and are then out of scope of the present document, and the present document has not been subject to any legal review.

Table B.1: Electronic signature context

Regulation recital 51	EU SSASC policy reference
*"It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that **appropriate mechanisms and procedures** are implemented to ensure that the signatory has **sole control over the use of his electronic signature creation data**, and the qualified electronic signature requirements are met by the use of the device".*	SIG-A.6-01: signature activation data format. SIG-A.6-02: signature activation data collection and generation. SIG-A.6-03: signature activation data parameters. SIG-A.6-04: signature activation data usage. SIG-A.6-05: signature activation data destination. SIG-A.6-06: signature activation data collection and protection. SIG-A.6-07: signature activation data submission under sole control. SIG-A.6-08: signature activation data protection after activation.
Regulation recital 52	**EU SSASC policy reference**
*"The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply **specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels,** in order to guarantee that the electronic signature creation **environment is reliable and is used under the sole control** of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply".*	SIG-A.5-03: cryptographic strength. SIG-A.5-04: threats mitigation. SIG-A.5-05: environment protection. SIG-A.5-06: protection against tampering. SIG-A.5-07: protection against attacker.

Regulation annex II Requirements for qualified electronic signature creation device	EU SSASC policy reference
"1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least: *(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;* *(b) the electronic signature creation data used for electronic signature creation can practically occur only once;* *(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;* *(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others".*	GEN-A.4-01: signing keys generated in a QSCD. GEN-A.4-02: QSCD configuration and operation.
"2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing."	SIG-A.5-01: signing keys used in a QSCD. SIG-A.5-02: QSCD configuration and operation.
"3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider".	OVR-A.1-01: SSASP as a Qualified TSP.
"4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met: *(a) the security of the duplicated datasets must be at the same level as for the original datasets;* *(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service".*	GEN-6.3.3-02: backup protection. GEN-6.3.3-04: backup minimum datasets.

Table B.2: Electronic seal context

Regulation recital 51	EU SSASC policy reference
"It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that ***appropriate mechanisms and procedures*** *are implemented to ensure that the signatory has* ***sole control over the use of his electronic signature creation data****, and the qualified electronic signature requirements are met by the use of the device".*	In the context of electronic seals, the term "sole control" is to be interpreted as "control". SIG-A.6-01: signature activation data format. SIG-A.6-02: signature activation data collection and generation. SIG-A.6-03: signature activation data parameters. SIG-A.6-04: signature activation data usage. SIG-A.6-05: signature activation data destination. SIG-A.6-08: signature activation data protection after activation.
Regulation recital 52	**EU SSASC policy reference**
"The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply ***specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels,*** *in order to guarantee that the electronic signature creation* ***environment is reliable and is used under the sole control*** *of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply".*	In the context of electronic seals, the term "sole control" is to be interpreted as "control". SIG-A.5-03: cryptographic strength. SIG-A.5-04: threats mitigation. SIG-A.5-05: environment protection. SIG-A.5-06: protection against tampering. SIG-A.5-07: protection against attacker.

Regulation annex II Requirements for qualified electronic signature creation device	EU SSASC policy reference
"1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least: *(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;* *(b) the electronic signature creation data used for electronic signature creation can practically occur only once;* *(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;* *(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others".*	GEN-A.4-01: signing keys generated in a QSCD. GEN-A.4-02: QSCD configuration and operation.
"2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing".	SIG-A.5-01: signing keys used in a QSCD. SIG-A.5-02: QSCD configuration and operation.
"3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider".	OVR-A.1-01: SSASP as a Qualified TSP.
"4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met: *(a) the security of the duplicated datasets must be at the same level as for the original datasets;* *(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service".*	GEN-6.3.3-02: backup protection. GEN-6.3.3-04: backup minimum datasets.

Annex C (informative): Scope of remote signing standards

C.1 Scope of remote signing standards

Figure C.1 illustrates the different standards applicable for a remote signature creation service.

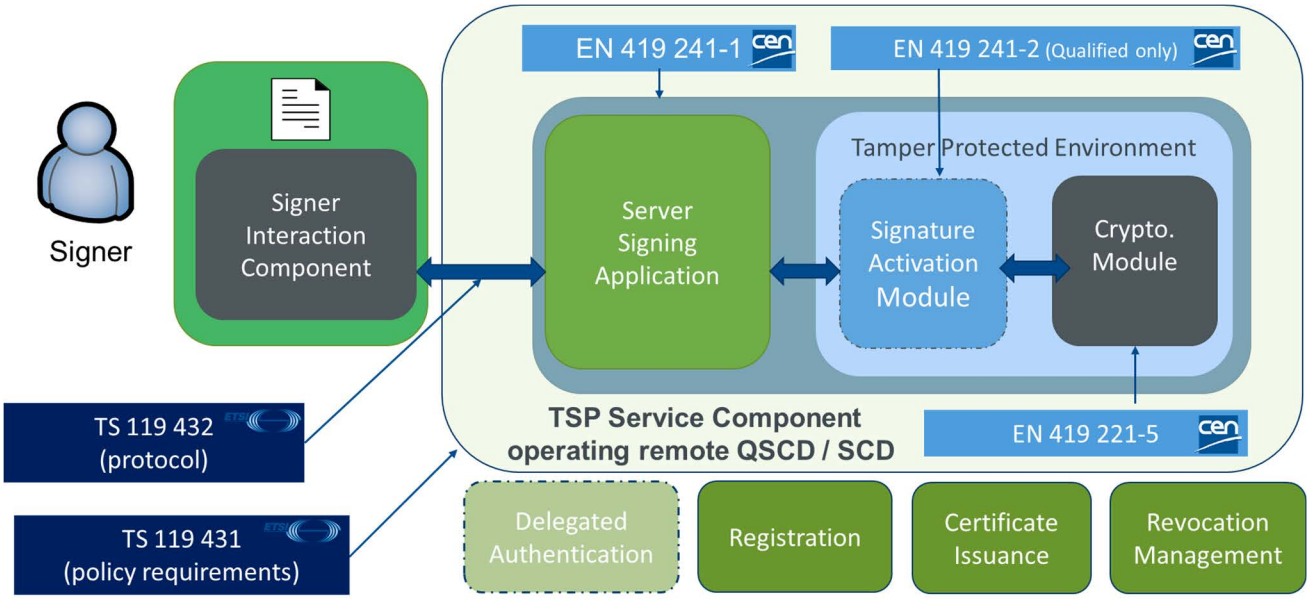

Figure C.1: Scope of standards on the different remote signing components

History

Document history		
V1.1.1	December 2018	Publication