CONNECTIVE

Connective -
Signature Validation Service Policy
version 1.0

This document describes which policy requirements are implemented by the default Connective Signature Validation Service.

creating trust connecting value

Connective Belgium
Wapenstraat 14 B301
2000 Antwerpen
T +32 3 612 58 60
www.connective.eu

Connective France
104 Avenue Albert 1er
92500 Rueil Malmaison
T +33 1 47 10 04 67
www.connective.eu

Connective The Netherlands
Zuid Hollandlaan 7
2596 AL Den Haag
+31 85 888 01 08
www.connective.eu

Revisions

Date	Owner	Topic
2018-12-12	JVH	Initial version 0.1
2019-01-07	FVE	Finalizing the document

CONNECTIVE

Table of content

Preface

This document describes the requirements that are being followed for the default Connective Signature Validation Service.

This document is structured as described by 'Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents' (ETSI TS 119 172-1 V1.1.1).

1. Introduction

1.1. Overview

This service receives signed data and signatures from the Driving Application (DA) from a service provider via an Application Programming Interface (API) and performs signature validation on the received signatures.

1.2. Business or Application Domain

1.2.1. Scope and boundaries of signature policy

This signature validation service does not pose any limitations on the scope and boundaries in which the signature validation service policy(ies) is(are) suitable for use.

1.2.1. Domain of applications

This signature validation service policy does not pose any limitation on the business (application) domain in which the signature is created.

1.2.2. Transactional context

This signature validation service policy does not pose any limitation on the transactional context in which the signature is created. See also clause 3.1.

1.3. Document and policy(ies) names, identification and conformance rules

1.3.1. Signature policy document and signature policy(ies) names

Signature validation policy name: Connective - Signature Validation Service Policy

1.3.2. Signature policy document and signature policy(ies) identifier(s)

Unique identifier: 1.2.528.56.1004.3.1.1.1 (OID)

OID hierarchy :

{
iso(1)
member-body(2)
nl(528)
belgium-organization(56)
connective(1004)
compliance-domain(3)
signature-validation-service(1)
practice-statement(1)
default-validation-policy(1)
}

1.3.3. Conformance rules

This document is structured as described by 'Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents' (ETSI TS 119 172-1 V1.1.1).

1.3.4. Distribution points

The latest version of this policy will always be present at
https://cdn.connective.eu/legal/Connective - Signature Validation Service Policy.pdf
Older version of this policy will be present on https://cdn.connective.eu/legal/archive/.

At this moment no machine processable formats are available for the signature policy related to this signature validation service policy.

1.4. Signature policy document administration

1.4.1. Signature policy authority

The Connective TSP Board is the authority that is responsible for the signature validation service policy document and the signature validation policy(ies) it covers. The Connective TSP Board is part of Connective NV (registered under number 0467.046.486 in Belgium).

The Connective TSP Board can be contacted via the contact form on the Connective website at https://connective.eu/contact/ or via e-mail at tsp-board@connective.eu or via postal mail at Connective TSP Board; Connective NV; Wapenstraat 14 bus 301, 2000 Antwerp.

It shall also provide information identifying the public key certificate corresponding to the private key used by the Connective TSP Board to digitally sign the Connective - Signature Validation Service Policy.

1.4.2. Contact person

Questions about this signature validation service policy should be addressed to the president of the Connective TSP Board.

This can be done via the contact form on the Connective website at https://connective.eu/contact/ or via e-mail at tsp-board@connective.eu or via postal mail at Connective TSP Board; Connective NV; Wapenstraat 14 bus 301, 2000 Antwerp.

1.4.3. Approval procedures

The approval procedures for this signature validation service policy consists of a formal approval by the members of the Connective TSP Board during a meeting or via an e-mail procedure.

1.5. Definitions and Acronyms

1.5.1. Definitions

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

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

eIDAS regulation: Regulation (eu) no 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

connective qualified signature validation service: the qualified signature validation service offered by Connective

qualified validation service for qualified electronic signatures: as specified in Regulation (EU) No 910/2014 [i.1], Article 33

relying party: natural or legal person that relies upon the signature validation service

service provider: a vendor that provides IT solutions and / or services to end users and organizations

shall: is to, is required to, it is required that, has to, only ... is permitted, it is necessary

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

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

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

signature validation application: application that validates a signature against a signature validation policy, consisting of a set of validation constraints and that outputs a status indication (i.e. the signature validation status) and a signature validation report

signature validation policy: list of constraints processed by the signature validation application

signature validation report: comprehensive report of the validation provided by the signature validation application to the driving application and allowing the driving application to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the signature validation application

signature validation service policy: set of rules indicating the applicability of a signature validation service to a particular community and / or class of application with common security requirements

signature validation status: TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE

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

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

signer: entity being the creator of a digital signature

subscriber: legal or natural person bound by agreement with Connective to any subscriber obligations. In the Connective ecosystem, subscribers consist as well from customers (service providers) that have signed a contract with Connective as end-users who only have accepted the terms and conditions of the services they are using

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

validation of qualified electronic signature: validation as specified in Regulation (EU) No 910/2014 [i.1], Article 32

validation of qualified electronic seals: validation as specified in Regulation (EU) No 910/2014 [i.1], Article 40

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

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

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

1.5.2. Acronyms

Acronym	Acronym for
AdES	Advanced Electronic Signature

AdES/QC	Advanced Electronic Signature created with a Qualified Certificate
ASiC	Associated Signature Containers
BSP	Business Scoping Parameter
CA	Certificate Authority
CAdES	Cryptographic Message Syntax Advanced Electronic Signature
DA	Driving Application
ESI	Electronic Signatures and Infrastructures
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAdES	Portable Document Format Advanced Electronic Signature
PKI	Public Key Infrastructure
QES	Qualified Electronic Signature
QTSP	Qualified Trust Service Provider
QSCD	Qualified Signature Creation Device
SCA	Signature Creation Application
SD	Signed Document
SDO	Signed Data Object
SSCD	Secure Signature Creation Device
SVA	Signature Validation Application
SVR	Signature Validation Report
SVS	Signature Validation Service
TSP	Trust Service Provider
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language

2. Signature Application Practice Statement

Please refer to the document ‘Connective – Signature Validation Service Practice Statement‘ with OID 1.2.528.56.1004.3.1.1

3. Business Scoping Parameters

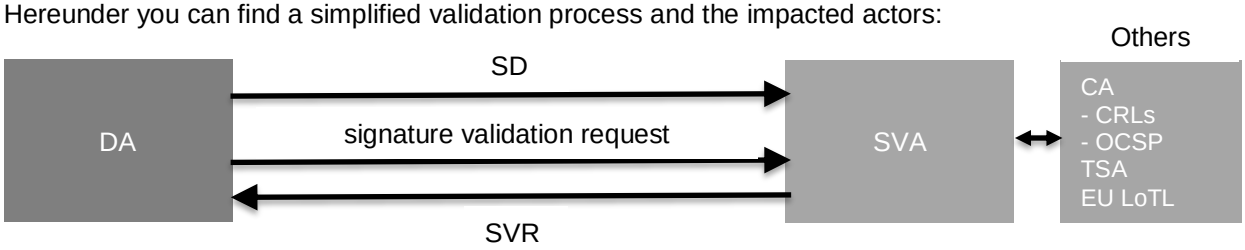
3.1. BSPs mainly related to the concerned application / business process

3.1.1. BSP (a): Workflow (sequencing and timing) of signatures

The SVA will treat every uploaded SD as a single unit of work. No workflow mechanism (for serial / parallel processing) is supported.

A single SD can however contain multiple signatures. This will then result in a single SVR containing all results of every single signature.

Hereunder you can find a simplified validation process and the impacted actors:



The SVA will perform the validation according to the validation algorithm defined in ESI - Procedures for Creation and Validation of AdES Digital Signatures (ETSI EN 319 102-1 V1.1.1).

Next is an indication of the supported signature sequencing possibilities per signature format:

Signature Format	Parallel	Serial	Counter	Combination
CAdES	☑	☑	☑	☑
PAdES	☒	☑	☒	☒
XAdES	☑	☑	☑	☑
ASiC	☑	☑	☑	☑

3.1.2. BSP (b): Data to be signed

Signature Format	Supported ETSI standards	Version
CAdES	ETSI TS 103 173 ETSI EN 319 122-1	v2.1.1 v1.1.1
PAdES	ETSI TS 103 172 ETSI EN 319 142-1	v2.1.1 v1.1.1
XAdES	ETSI TS 103 171 ETSI EN 319 132-1	v2.1.1 v1.1.1
ASiC	ETSI TS 103 174 ETSI EN 319 162-1	v2.1.1 v1.1.1

3.1.3. BSP (c): The relationship between signed data and signature(s)

Levels of signatures as defined in ETSI standards on signature formats address incremental (augmenting) requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it.

Based on this augmented data, the level of signature will be determined and will be indicated in the SVR.

3.1.4. BSP (d): Targeted community

No specific validation policy rules per community are in place.
Every registered subscriber of the SVS will use the same validation policy rules.

3.1.5. BSP (e): Allocation of responsibility for signature validation and augmentation

This signature validation service policy is not limited to a certain application or business process. The DA is responsible for all business aspects. This validation service policy does not impose the validation of any signature applicability rules. If the application or business process needs the verification of signature applicability rules, it is the responsibility of the service provider that operates the DA to perform such verification.

In case there are multiple signatures on the signed data, the SVA shall include a validation result about each signature it was able to detect in the SVR. However the SVA is not necessarily able to detect all types of electronic signatures (e.g. it cannot detect non-advanced electronic signatures). As such, it is the responsibility of the service provider to verify whether all signatures that are supposed to be present on the signed data are indeed covered by the SVR.

The validation report will indicate, per signature, the signature validation status: TOTAL-PASSED, INDETERMINATE, TOTAL-FAILED.

This signature validation service policy does not foresee signatures to be augmented during or after the validation process. Signature augmentation, preservation and archival are the responsibility of the service provider.

3.2. BSPs mainly influenced by the legal / regulatory provisions associated to the concerned application / business process

3.2.1. BSP (f): Legal type of the signatures

The SVR shall specify whether the validated signature concerns:

- a qualified electronic signature (QESig) *or*
- an advanced electronic signature supported by a qualified certificate (AdESig-QC) *or*
- an advanced electronic signature (AdESig) *or*
- a qualified electronic seal (QESeal) *or*
- an advanced electronic seal supported by a qualified certificate(AdESeal-QC) *or*
- an advanced electronic seal (AdESeal)

If the SVA could not determine the type of signature, 'Not applicable' (N/A) will be returned. The SVR will in that case also elaborate on why it could not determine the type of signature.

3.2.2. BSP (g): Commitment assumed by the signer

In case a commitment type is indicated in the signature, the SVR will mention this commitment.

All commitment types, as defined in TS 101 733 - V2.2.1 - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES) (Clause 5.11.1), are supported.

Commitment types are however not required.

3.2.3. BSP (h): Level of assurance on timing evidences

The SVR will indicate whether timestamps were used to determine the best signature time.
It will however not differentiate between qualified and non-qualified timestamps.

See section 0 for more information on the approach towards signing time.

3.2.4. BSP (j): Longevity and resilience to change

The SVR does not give any indication on the expected longevity and resilience to change of the signature.

3.2.5. BSP (k): Archival

It is the responsibility of the service provider to archive the SVR if needed.

3.3. BSPs mainly related to the actors involved in creating / augmenting / validating signatures

3.3.1. BSP (l): Identity (and roles / attributes) of the signers

In case a signer role / attribute is indicated in the signature the SVR will mention this role / attribute.

3.3.2. BSP (m): Level of assurance required for the authentication of the signer

The SVR will not give an indication on the level of assurance for the identity of the signer. But of course due to the indication on the level (qualified or not) of the signers certificate, the relying party has an indication about this via that parameter.

3.3.3. BSP (n): Signature creation devices

The SVR only gives indications about the signing creation devices if the signature contains a Qualified Electronic Signature (in that case the private key was protected by a QSCD). In other cases it does not give any indication about the use of a Signature Creation Device for the protection of the private key.

3.4. Other BSPs

3.4.1. BSP (o): Other information to be associated with the signature

If applicable, the following information will be taken up in the SVR:

- ContentType
- ContentIdentifier
- ContentHints
- SignatureProductionPlace
- SignaturePolicy
- Pseudonym

3.4.2. BSP (p): Cryptographic suites

The SVR will indicate the cryptographic algorithms and key lengths that were used for cryptographic operations, it will however not indicate whether the algorithm and key lengths were still trustworthy at the time of use.

The following encryption algorithms are supported (with the minimal public key length):

- RSA (128-bit)
- DSA (1024-bit)
- ECDSA (192-bit)

The following digest algorithms are supported:

- SHA1
- SHA224
- SHA256
- SHA384
- SHA512
- SHA3-224
- SHA3-256
- SHA3-384
- SHA3-512
- RIPEMD160

3.4.3. BSP (q): Technological environment

The signature validation service will be accessible only via a REST API. This makes the constraints on operating system, programming language, etc. irrelevant.

Communication between DA and SVA *shall* be done through MTLS connections, which is supported but technically not enforced.

4. Requirements / statements on technical mechanisms and standards implementation

4.1. Technical counterparts of BSPs - Statement summary

This signature validation policy will validate electronic signatures and indicate whether they are Advanced Electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified Electronic Signature (QES).

All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).

To determine the certificate qualification, the SVA follows the standard Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists (ETSI TS 119 172-4). It analyses the certificate properties and applies possible overrules from the related trusted list.

The SVS will always computes the status of the certificate for two different times: certificate issuance and signing / validation time. This is a necessity since the certificate qualification can evolve over time. The eIDAS regulation clearly defines these different times in the Article 32 and related Annex I.

4.1.1. Approach towards signing time

The signing time against which the validity of the signature will be verified will be defined as follows:

1. The signing time will be attempted to be defined based on a Proof of Existence (e.g. timestamp or evidence record) present in the signature.

2. If such Proof of Existence is not available (e.g. no proof of existence can be extracted from the signature), *and* the DA has indicated a time that should be used as signing time, this time indication will be used. See section 4.2.1 on how this date should be provided.

3. In absence of a Proof of Existence and indication from the DA, the signing time will be set to the validation time (current time).

NOTE: The embedded (claimed) signing time is never used.

4.1.2. Defining the qualified status of a signature or seal

In order to define whether a signature or seal is a Qualified Electronic Signature or a Qualified Electronic Seal with a private key residing in a QSCD, the following verifications will be performed by the SVA.

4.1.2.1. Defining the list of trusted services for the signing or sealing certificate

The validation service will verify whether the signing or sealing certificate can be chained to a trust anchor that is indicated on a EU Member State Trusted List (TL).

In order to do so, the TLs will be downloaded on a regular basis and the validity of the TLs will be verified (signature on the TL and expiration).

The trusted services defined in these TLs will then be filtered according to the signing / sealing certificate's root anchor and it will be verified that the trust anchor is listed with the correct service type (CA for Qualified Certificates) and service status statements.

4.1.2.2. Defining the qualified status of the signing or sealing certificate

In order to verify if the signing or sealing certificate is a Qualified Certificate, the use of '*QcCompliance*' statement and the corresponding information of the applicable EU Member State Trusted List will be

verified. The list of trusted services that are the result of the process defined in section 4.1.2.1 are further filtered based on the dates that should be checked. The dates of importance are:

- The signing certificate's issuance time *and*
- the signing time as defined in 0.

The captured qualifiers of the selected trusted service (for the certificate and dates) are checked in case they exist.

If no selected trusted service is found, the signing or sealing certificate is considered *not* qualified.

NOTE: The result of the TL takes precedence over the information in the certificate.

4.1.2.3. Defining whether the private key resides in a QSCD

In order to verify if the private key is protected on a QSCD, the presence of SSCD or QSCD statement in the certificate will be verified.

The list of trusted services that are the result of the process defined in section 4.1.2.1 are further filtered based on the dates that should be checked. The dates of importance are:

- The signing certificate's issuance time *and*
- the signing time as defined in 0.

The captured qualifiers of the selected trusted service (for the certificate and dates) are checked for SSCD or QSCD statement in case they exist.

If no selected trusted service is found, the private key is considered *not* QSCD.

NOTE: The result of the TL takes precedence over the information in the certificate.

4.1.2.4. Defining the type of the signature / seal

The type of signature/seal will be determined based on the presence of the combination of QC and SSCD or QSCD statements in the certificate.

The list of trusted services that are the result of the process defined in section 4.1.2.1 are further filtered based on the date that should be checked. The dates of importance are:

- The signing certificate's issuance time *and*
- the signing time as defined in 0.

The captured qualifiers of the selected trusted service (for the certificate and dates) are checked in case they exist for Service Info Extension statements that indicate a QC.

If no selected trusted service is found, the type as defined in the certificate is returned.

NOTE: The result of the TL takes precedence over the information in the certificate.

4.1.2.5. Defining type consistency between certificate and TL

In case the trusted service has no Service Info Extension statements that indicate a QC, the presence of *'Additional Service Information'* extensions are checked and need to be consistent with the defined type in the certificate.

4.2. Input and output constraints for signature creation, augmentation and validation procedures

4.2.1. Input constraints to be used when generating, augmenting and / or validating signatures in the context of the identified signature policy

4.2.1.1. Validation time

As explained in section 0, the DA can provide a validation time in the signature validation request. This can be done by making use of the 'verifyDate' property of the request.

4.2.1.2. Validation process

The DA can also specify the validation process that should be performed by the SVA by providing a value for the 'verifyLevel' property of the request.

Possible values are:

- BASIC_SIGNATURES: corresponding to ETSI TS 119 102-1 clause 5.3
- LONG_TERM_DATA: corresponding to ETSI TS 119 102-1 clause 5.5
- ARCHIVAL_DATA (default): corresponding to ETSI TS 119 102-1 clause 5.6.3

4.2.2. Output constraints to be used when validating signatures in the context of the identified signature policy

The SVR will be formatted in XML.

Depending on the value of 'verifyReport' in the signature validation request, either a simple, detailed, diagnostic or concatenated report is being generated.

The XSD's of these XML reports can be found here:

- https://cdn.connective.eu/legal/documentation/SimpleReport.xsd
- https://cdn.connective.eu/legal/documentation/DetailedReport.xsd
- https://cdn.connective.eu/legal/documentation/DiagnosticData.xsd

The concatenated report does not have a specific XSD, it is nothing more than the combination of the simple, detailed and diagnostic report.

4.2.3. Output constraints to be used for generating / augmenting signatures in the context of the identified signature policy

Not applicable.

5. Other business and legal matters

This signature validation service policy does not impose or implement any business matters. All legal matters are governed by the contract or Terms and Conditions that were accepted by the subscriber before starting to make use of the signature validation service.

6. Compliance audit and other assessments

This signature validation service policy is a policy for the Connective Signature Validation Service, which is a Signature Validation Service.

This service is subject to the rigorous eIDAS accreditation scheme.

No other compliance audits or assessments are applicable.