CONNECTIVE

Connective Trust Service Practice Statement

version 1.2

This document describes what practices are in place for the provisioning of the Connective Trust Services.

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
Evert van de Beekstraat 360
1118 CZ Schiphol
T +31 85 888 20 70
www.connective.eu

Connective Spain
C/ Marina 16-18 | 27th floor
Barcelona, 08005
T +34 518 899061
www.connective.eu

Revisions

Date	Version	Owner	Topic
2018-12-18	v0.1	JVH	Initial version
2019-01-04	v1.0	Filip Verreth	Finalize document
2019-01-04	v1.1	Filip Verreth	eIDAS alignment – adapt references - add clarifications
2020-12-03	V1.2	Wim Coulier	Expand scope, alignment with ETSI standards and rename document name

CONNECTIVE

Table of content

Preface

This document describes what practices are in place for the provisioning of the default Connective Trust Services.

The document is structured as described by Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services (ETSI TS 119 441 V1.1.1) Annex A.

1. Introduction

1.1. Overview

1.1.1. TSP identification

Practice statement name: Connective Trust Service Practice Statement

Unique identifier: 1.2.528.56.1004.4.1 (OID)

OID hierarchy :

{
iso(1)
member-body(2)
nl(528)
belgium-organization(56)
connective(1004)
TSP-domain(4)

connective-trust-services-practice-statement (1)
}

1.1.2. Supported signature validation service policy(ies)

This Trust Service Practice Statement is applicable to Connective - Signature Validation Service Policy with OID 1.2.528.56.1004.4.2

1.1.3. Supported signature creation service policies

This Trust Service Practice Statement is applicable to Connective - Signature Creation Service Policy with OID 1.2.528.56.1004.4.3.

1.2. Signature Validation Service Components

1.2.1. SVS actors

driving application (DA): application that uses an SVS in order to validate digital signatures

Signature Validation Application (SVA): application that validates a signature against a signature validation policy, and that outputs a status indication

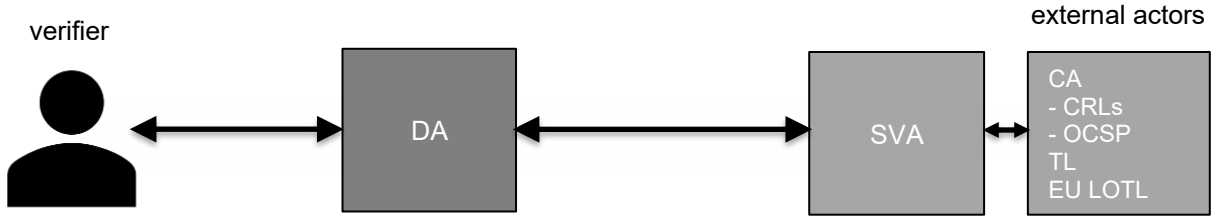
verifier: an entity interacting with the driving application and that wants to validate or verify a digital signature

external actors:

- Trust Service Provider (TSP) having issued the signer's certificate (Certificate Authority)
- European trusted list providers
- European Commission providing the List of Trusted Lists

1.2.2. Service architecture

Hereunder you can find a simplified architecture and the involved actors:



User:

- selects the signed data to be validated
- uses the validation response or report

Note: in case of automated process the user can be a system instead of a human being

DA (provided by the Subscriber):

- builds the signature validation request
- communicates with the SVA to obtain the validation response or report
- when applicable, cares for the validation report presentation
- can incorporate:
  - a user interface for manually inputting the request
  - a machine interface for automated requests
  - a user interface to present the report

SVA (provided by Connective):

- communicates with the DA to receive validation requests
- implements the validation algorithm to define the signature validation status
- can call external actors to obtain required information during the execution of the validation algorithm
- creates the SVR related to the request
- builds and returns the signature validation response

1.3. Signature Creation Service Components

Note: Seal creation is seen as a special case of signature creation. The “signer” is then a legal entity. In case that the seal is created by a natural person for a legal entity (e.g. certificate of the legal entity on a smartcard operated by a human representative), the schema is exactly the same as for signature creation. However, seal creation can also be performed without human involvement where a system requests the seal creation in the name of the legal entity. ***

1.3.1. SCS actors

Certificate Authority (CA): authority trusted by one or more users to create and assign public-key certificates

driving application (DA): application that uses an SVS in order to validate digital signatures

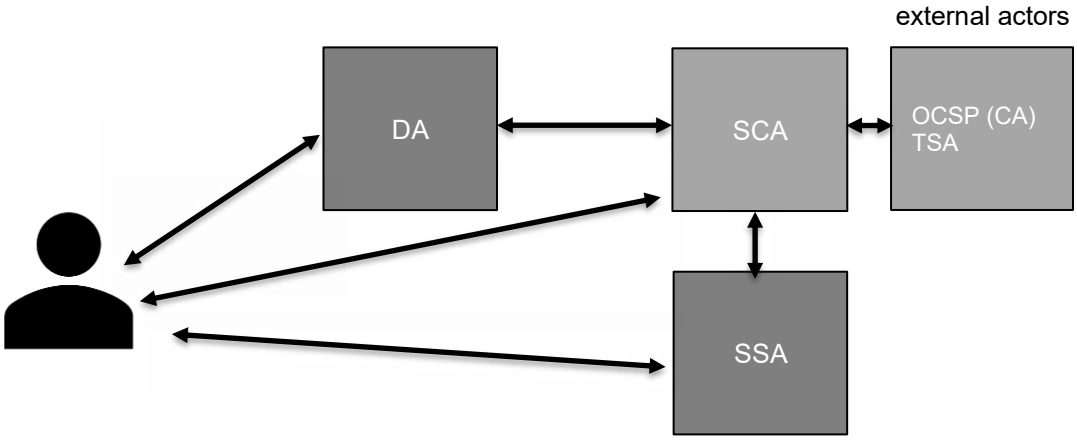
Server Signing Application (SSA): application using a remote signature creation device to create a digital signature value on behalf of a signer

Signature Creation Application (SCA): the application that creates a signature data object

Signer: entity being the creator of a digital signature

Timestamping Authority (TSA): trust service provider which issues time-stamps

1.3.1. Service architecture



Initiator:

- selects the data (document) to be signed (note: this can be in a DA provided by the subscriber or directly in the Connective SCA)
- selects the signer(s) and the signing sequence
- potentially selects the receivers of the signed data

Signer

- views the data to be signed on the SCA
- activates the signature creation device with his sole control mechanism (note: the actual sole control mechanism is depending on the signing method being used)

DA (optional, provided by the subscriber):

- builds the signature creation request
- communicates with the SCA to provide the data to be signed, the signer(s) and potentially the receivers
- can incorporate:
  - a user interface for manually inputting the signing request
  - a machine interface for automated requests
  - a user interface to present the signed data

SCA:

- in case the signer acts via a DA: communicates with the DA to receive signature creation requests
- visualizes the data to be signed to the signer
- interacts with the signature creation device and requests the user to active the signing key with his sole control mechanism
- receives the raw signature from the signature creation device
- calls external actors to obtain proofs of validity (OCSP responses, timestamps, …)
- creates the AdES formatted signature
- delivers the signed data to the indicated receivers and to the signers and/or DA

SSA (optional):
Note: the SSA is provided by an external provider

- the SSA is triggered by the SCA at the time the raw signature needs to be created
- the user is requested to use his sole control mechanism to activate the private key in the RQSCD of the SSA (note: in the case of seal creation, the user can be either a human being

or a system)
- the SSA has the raw signature created in its RQSCD and returns it to the SCA

1.4. Definitions and Acronyms

1.4.1. Definitions

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

proof of existence: evidence that proves that an object existed at a specific date/time

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

signature validation application: an 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

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

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

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

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

1.4.2. Acronyms

Acronym	Acronym for
AdES	Advanced Electronic Signature
AdES/QC	Advanced Electronic Signature created with a Qualified Certificate
CA	Certificate Authority
CRL	Certificate Revocation List
DA	Driving Application
ESI	Electronic Signatures and Infrastructures
LOTL	List Of Trusted Lists
OCSP	Online Certificate Status Protocol
OID	Object Identifier
POE	Proof Of Existence
QES	Qualified Electronic Signature
QTSP	Qualified Trust Service Provider
R(Q)SCD	Remote (Qualified) Signature Creation Device
SCA	Signature Creation Application
SCASP	Signature Application Service Provider
SCS	Signature Creation Service
SD	Signed Document
SSA	Server Signing Application
SVA	Signature Validation Application
SVR	Signature Validation Report
SVS	Signature Validation Service
SVSP	Signature Validation Service Provider
TSA	Timestamping Authority
TSP	Trust Service Provider
XML	eXtensible Markup Language

1.5. Policies and practices

1.5.1. Organization administrating the TSP documentation

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

The approval procedures for this Trust Service Practice Statement consists of a formal approval by the members of the Connective TSP Board during a meeting or via an e-mail procedure.

In order of notify notice of changes, any new version of the Connective Trust Service Practise Statement will be published at least two weeks before it becomes applicable. This period might be shortened or even skipped altogether in case of urgent changes (e.g. changes affecting security).

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.

Connective TSP policy documents, amongst which the current Connective TSP Services Practice Statement, are signed by the CEO of Connective (Nicolas Metivier) in order to provide proof of origin and integrity.

1.5.2. 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.

1.5.3. TSP (public) documentation applicability

The latest version of this practice statement will always be present at:
https://connective.eu/about/trust-center/compliance/

The latest version of the Terms of use applicable to the Validation Service will always be present at :
https://connective.eu/about/trust-center/compliance/

The terms and conditions of the signature creation service is part of the contract that is signed by the Service Providers.

Older version of this practice statement will be present on https://connective.eu/about/trust-center/compliance/

2. Trust Service management and operation

2.1. Internal organization

2.1.1. Organization reliability

2.1.1.1. Connective's obligations

Connective offers its Trust Services under non-discriminatory practices.

Connective ensures that all requirements defined in this Practice Statement are implemented and remain applicable to the Trust Services provided.

Connective complies with all legal obligations applicable to the provisioning of its Trust Services.

Connective fulfills general security requirements set out in article 19 of the eIDAS Regulation as further developed in ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

In relation to the signature validation Trust Services, Connective provides validation of (Qualified) Electronic Signatures and Seals in accordance with article 32 of the eIDAS Regulation and relevant sections of "ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services" and "ETSI TS 119 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

The Signature Creation Service is provided in accordance with the applicable sections of the eIDAS Regulation, namely Recitals (52, 55) and Annex II.3 and relevant sections of "ETSI TS 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" and "ETSI TS 119 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

The provision of Trust Services is subject to an external audit performed at least every 24 months by a Conformity Assessment Body and the qualified status is supervised by the Supervisory Body appointed by FOD Economics.

Records concerning the operation of the Trust Services are made available to affected parties upon legitimate request for the purposes of providing evidence of the correct operation of the Trust Services for the purposes of legal proceedings.

2.1.1.2. Subscriber obligations

Subscribers are obliged to maintain confidentiality of passwords and applicable credentials to use the Validation Services and promptly communicate to Connective any circumstance raising suspicion or risk of them being compromised.

2.1.1.3. Obligations of all external organizations

Certification Authorities supporting the Trust Services are subject to the fulfillment of applicable obligations under Regulation (EU) 910/2010.

An external supplier providing data center collocation services to Connective is responsible for ensuring business continuity, as well as physical security and monitoring systems alerting any attempt of unauthorized access to its perimeter. Connective monitors implementation of applicable controls on a regular basis.

The subscriber obligations are taken up in the terms and conditions.

Each third party TSP is responsible for the service it delivers.

2.1.1.4. Connective's liability

Connective is liable for the performance of all its obligations to the extent prescribed by the legislation of Belgium.

Connective has appropriate insurance arrangements to cover Connective provision of Trust Services to ensure compensation for damages caused by an intentional or negligent violation of Connective obligations under the eIDAS Regulation.

Connective is not liable for:

- Any damage arising from a signatory or a Subscriber failing to maintain the secrecy of the OTP devices, passwords and applicable credentials to use the Signature Service or the Trust Services
- The non-performance of its obligations if such non-performance is due to faults or security problems of any public authority
- Non-fulfillment of its obligations if such non-fulfillment is caused by a Force Majeure event.

2.1.1.5. Dispute resolution

Disputes related to Trust Services provided by Connective shall be settled initially through a conciliation procedure, during which both Parties shall in good faith negotiate solutions in respect of any disputes arising. Connective's TSP Board shall be responsible for handling such conciliation procedure. If the specific complaint is not settled within thirty (30) days of the commencement of the conciliatory process, the Parties may refer the dispute to the appropriate courts of Antwerp, department Antwerp.

2.1.1.6. Confidentiality

All confidential and proprietary information disclosed to Connective in the use of Trust Services shall be Confidential Information.

Confidential Information does not include information that:

- enters the public domain through no fault of Connective;
- is communicated by a third party to Connective free of any obligation of confidence;
- has been independently developed by Connective without reference to any Confidential Information of the disclosing party;
- was in Connective's lawful possession prior to disclosure and had not been obtained either directly or indirectly from the disclosing party, *or*
- is required to be disclosed by law, provided Connective has promptly notified the disclosing party in writing of such requirement and allowed the disclosing party a reasonable time to oppose such requirement.

2.1.2. Segregation of duties

Strict segregation of duties between development and operation of the platform is ensured organizationally and is being implemented technically. Security administration and operation roles are not organizationally segregated but are strictly restricted to authorized personnel (a few system administrators).

2.2. Human resources

2.2.1. Reliability

Connective as a trusted service provider makes or ensures that the relevant checks are performed to prospective personnel.

For restriction of access to privileged operations, we refer to section 7.4.
Basic obligations with regards to security are set out in each person's working agreement: this includes confidentiality and non-compete clauses in contract.

We additionally refer to Chapter 6 on security policies for information related to definition and enforcement of security policies.

2.2.2. Confidentiality

Our core activities consist of ICT solutions and services. That means that every colleague has (to a certain extent) access to the intellectual property of Connective and to our Clients' sensitive business information. Each employee is therefore required to sign a confidentiality agreement in which he/she expressly undertakes to respect and protect the secrecy of the intellectual property and the business information of Connective and of its Clients. Provision of Trust Services entails the possibility that employees will come into contact with personal data and/or information of a private nature of the Users of the Services. It is for that reason that the confidentiality agreement is made all the more stringent for the protection of the privacy of our Users. Each employee will further give his/her consent as regards possible future changes to the confidentiality agreement, for application simply in connection with legal requirements or criteria imposed by the Supervisor and will sign the same on presentation. The employment contract may otherwise then be suspended or even terminated in accordance with the Employment Regulation. Furthermore, all provisions of the Employment Regulation and our corporate policy regarding the correct use of email, internet and social media remain fully effective.

2.2.3. Expertise, experience and qualifications

Each prospective employee is assessed for the necessary proofs of qualification of professional training necessary to carry out the function concerned in a proficient and qualitative manner. If sufficient experience has been acquired in the actual work environment and can represent the equivalent of a professional training course (or courses), the relevant requirements are clearly mapped out in the vacancy and will be checked by reference to the proofs of experience submitted by the prospective employee.

2.2.4. Suitable training

Connective staff is regularly trained on security by qualified specialized security professionals, such as specialized professors from the KUL (University of Leuven) and cyber security professionals.

Permanent training and ad hoc courses will be offered to keep our employees up-to-date and abreast of the latest developments in technology, security and the processing and protection of data and the legal aspects related to their work. Self-development, internal advancement, specialization and expansion of their field of knowledge are always encouraged and, wherever possible, supported by training courses, both internally and externally. It goes without saying that action will be taken in response to the offer of specific vocational training courses in the broader context of permanent training as required by the Supervisor.

2.3. Asset management

2.3.1. General requirements

A top down evaluation indicates that all systems should be considered critical, in that they may hold either customer data or Connective sensitive or personal data.

An inventory of all devices and the supporting owner is maintained; a similar but partial inventory is in place for software in use in the organization.

An 'Acceptable Use Policy' is in place that requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2.3.2. Media handling

Where media are managed by outsourcing parties, those parties have proper media handling processes and procedures in place. For any media managed by Connective, the Physical Security Policy foresees the proper handling of these media.

2.4. Access control

Connective operates a segmented network (users, development and production) where firewalls are in place.

Access to privileged operations are restricted by means of access controls, where a series of groups and profiles have been defined and assigned as per job responsibilities: these are designed to enforce segregation of duties and least privilege principle – we additionally refer to section 2.1.2 on segregation of duties.

Access rights are allocated after management authorization.

Data archiving and retention requirements are defined by the data controller, i.e. Connective's Customers.

2.5. Cryptographic controls

Data at rest and transit are encrypted using industry standards.

2.6. Physical and environmental security

Physical access to Connective offices & Azure data center facilities is appropriately restricted to authorized personnel. Safeguard measures are in place to protect critical assets and ensure continuity.

2.7. Operational security

In terms of Change Control, for every change or project to the Connective platforms, functional and technical analysis is conducted and includes an identification of appropriate security measures required. Changes are controlled by means a formal incident and change management process.

Anti-malware protection is enabled, and removable media use is limited, and does not support business critical activities.

Windows servers and SQL databases are automatically patched, leveraging default Azure functionalities. A patch management process is formally defined.

The maximum interval between two checks of violating changes on systems is one month (but the aim is to perform such checks on a weekly basis).

2.8. Network security

Network segmentation is enforced, as detailed in section 2.4.

For our Cloud services, Microsoft's platform as a service ensures appropriate secure configuration. Availability is similarly guaranteed by leveraging Azure mechanisms & data center protection. Information flows have been secured by means of encryption and are restricted between network segments.

2.9. Incident management

Logging leverages default Azure functionalities, both at host and account level. Log monitoring is performed reactively, to ensure analysis of anomalous behavior. A formal incident management process is defined, and dedicated information security incident management process: as part of GDPR implementation, procedures are defined.

2.10. Collection of evidence

Connective maintains records concerning the operation of the Trust Services for the purposes of providing evidence of the correct operation of the Trust Services. These records will only be disclosed to law enforcement authorities under court order and to persons with right to access to them upon legitimate request. These records are maintained under confidentiality in facilities to ensure availability throughout the period they are maintained.

2.11. Business continuity management

A business continuity and disaster recovery plan are in place.

2.12. TSP termination and termination plans

Before Connective terminates a Trust Service the following procedures will be executed:

- Connective informs the following parties about the termination: all subscribers and other entities with which Connective has agreements. In addition, this information will be made available to other relying parties (e.g. by publishing the notice of termination on Connective's website).

- Connective shall, if applicable, terminate authorization of all subcontractors to act on behalf of Connective in carrying out any functions relating to the trust services.

- Connective shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of Connective for a reasonable period, unless it can be demonstrated that Connective does not hold any such information.

- Connective's private keys, including backup copies, that are no longer required for other services or decryption of information to be maintained after termination, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

- To the extent required under the applicable regulations, Connective notifies the supervisory body of any change in the provision of its trust services and an intention to cease those activities.

2.13. Compliance

Connective has implemented the General Data Protection Regulation. Standards on availability to persons with disabilities is partially considered.

3. Signature validation service design

3.1. Signature validation process requirements

3.1.1. Signature validation process

Generally, and following Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation ETSI EN 319 102-1 V1.1.1, the validation process will provide, per validated signature, one of the three following status indications:

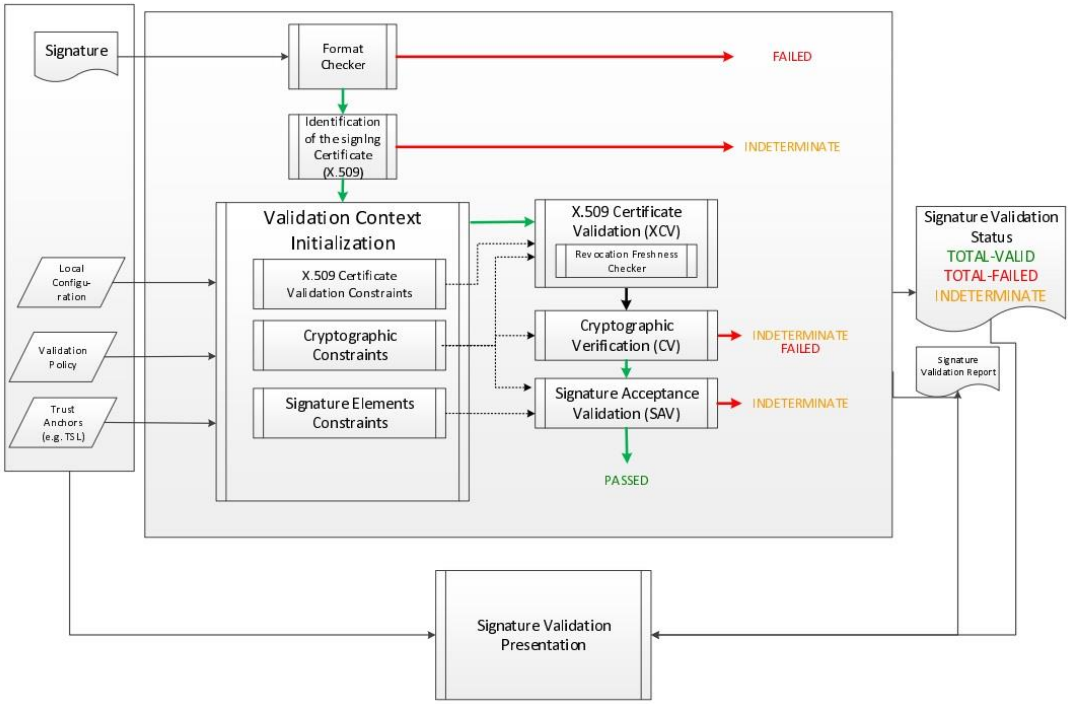
- TOTAL-PASSED: indicates that the signature has passed verification and it complies with the signature validation policy
- TOTAL-FAILED: indicates that either the signature format is incorrect or that the digital signature value fails verification
- INDETERMINATE: indicates that the format and digital signature verifications have not failed but there is insufficient information to determine if the electronic signature is valid

For each of the validation checks, the validation process provides information justifying the reasons for the resulting status indication as a result of the check against the applicable constraints. In addition, the ETSI standard defines a consistent and accurate way for justifying statuses under a set of sub-indications.

The validation process is driven by the validation policy and allows long term signature validation. It not only verifies the existence of certain data and their validity, but it also checks the temporal dependencies between these elements. The signature check is done following basic building blocks.

The SVS supports only one signature validation policy for the moment. The SVS does not accept other sources of validation policies. This means that the process is controlled by a set of validation constraints that are implicitly defined by the implementation itself. The implemented signature validation policy is a validation policy for validating that a signature is a qualified electronic signature or seal as per Regulation (EU) No 910/2014.

On the simplified diagram below, showing the process of the signature validation, you can follow the relationships between each building block which represents a logic set of checks used in the validation process.



The result of the validation process consists of three elements:

- the simple report (macroscopic view),
- the detailed report (microscopic view) *and*,
- the diagnostic data (input data).

These three reports can also be returned as one by the SVA, this is the *concatenated* report.

All these reports are encoded using XML, which allows the implementer to easily manipulate and extract information for further analysis.

3.1.2. EU Trusted Lists of Certification Service Providers

On 16 October 2009 the European Commission adopted a Decision setting out measures facilitating the use of procedures by electronic means through the "points of single contact" under the Services Directive. One of the measures adopted by the Decision consisted in the obligation for Member States to establish and publish by 28.12.2009 their Trusted List of supervised/accredited certification service providers issuing qualified certificates to the public. The objective of this obligation is to enhance cross-border use of electronic signatures by increasing trust in electronic signatures originating from other Member States. The Decision was updated several times since 16.10.2009; the last amendment was made on 01.02.2014. The consolidated version is available here for information.

In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission has published a central list with links to national "trusted lists" (LOTL).

The LOTL is published by the EU at the following URL : https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml. This XML file contains the list of the trusted list. This file must be signed by an allowed certificate. To know who has the permission to sign / publish the LOTL, we need to refer to the Official Journal Of the Union (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.233.01.0001.01.ENG).

If the LOTL signature is valid, the content can also be trusted. It contains some information for each country: URLs of the XML / PDF files, the allowed certificates to sign, … So, when trusting the LOTL, we can process each TL. If they are valid, we can trust the service providers and its certificates.

This LOTL is then used to perform the certificate validations that are needed in the context of a signature validation. The SVS builds the certificate path until a known trust anchor, validates each found certificate (using OCSP when possible, otherwise CRL) and determines its European "qualification".

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.

3.2. Signature validation protocol requirements

The signature validation protocol will be as follows:

1. the DA sends the SD containing the digital signature(s) to be validated to the SVS
2. the DA sends the signature validation request to the SVS
3. the SVS sends the signature validation response containing the SVR to the DA

It is not allowed to only send the hash in step 1. This would be a risk for the human end-user. If he receives the SVR via an intermediate that operates the DA, the DA could maliciously present a wrong report to the end-user, by providing a wrong hash to the SVS (e.g. deliver hash and signature of another validly SD to the SVSP and deliver the report on that to the end-user for a malicious document).

3.3. Interfaces

3.3.1. Communication channel

Communication between DA and SVS should occur via a secured MTLS connection. This will ensure confidentiality of the transmitted data and offer a way for both parties to authenticate each other.

3.3.2. SVSP - other TSP

Communication between the SVSP and other TSPs depend upon the interface that is defined and he requirements of the TSP that needs to be called.

The SVS however is foreseen to setup MTLS connections or other authentication means to communicate with external actors.

3.4. Signature validation report requirements

The result of the validation process consists of three elements:

- the simple report (macroscopic view)
- the detailed report (microscopic view)
- the diagnostic data (input data)

These three reports can also be returned as one by the SVS, this is named the *concatenated* report. In order to use the Connective SVS as a qualified service, the DA shall request the concatenated report.

All these reports are encoded using XML, which allows the implementer to easily manipulate and extract information for further analysis. No presentation whatsoever of the SVR is foreseen in the SVS. If this is a desired functionality, it is considered a responsibility of the SVC.

The simple report shall, amongst other information, contain the signer's identity. It shall also contain the status indication per validated signature, being:

- TOTAL-PASSED *or*
- TOTAL-FAILED *or*
- INDETERMINATE

The simple report shall also report on sub-indications as specified in ETSI TS 119 102-1.

The detailed report shall report on each of the validation constraints that is processed including any validation constraints that have been applied implicitly by the implementation. It shall also provide information on the validation process that has been used.

The diagnostic data shall report on signed attributes that were present in the signature. It will also contain any POE that was used during the validation process and indicate its origin and quality.

4. Signature creation application service component technical requirements

4.1. Interface

4.1.1. Communication channel

Communication between DA and SCS should occur via a secured MTLS connection. This will ensure confidentiality of the transmitted data and offer a way for both parties to authenticate each other.

4.1.2. SCSP - other TSP

Communication between the SCSP and other TSPs depend upon the interface that is defined and he requirements of the TSP that needs to be called.

The SCS however is foreseen to setup MTLS connections or other authentication means to communicate with external actors.

4.2. AdES digital signature creation

The algorithms being used will be algorithms recommended by ETSI TS 119 312. The hashing algorithm will be SHA256 or stronger. The signing algorithm for QES, is defined by what is supported by the QSCD.

Documents that are received are stored in a secure datacenter. The user chooses the signing certificate from the allowed signing methods. No authentication data passes to the SCA for any of the supported signing methods.

The SCA is able to ensure correct representation of PDF and XML content types. In the case of unstructured documents are used as input for the data to be signed, it will be converted by the SCA to PDF. It is this PDF that then will be signed in the PAdES format. The SCA will created PNG images of each page of the PDF and these PNG images are visualized in the browser of the user for the WYSIWYS experience. For XML documents the XML file itself is visualized to the user, but the signer can request to see the human readable form (PNG of a PDF). The human readable form is only available if the DA provides a human readable form in PDF for the XML. In case a specific signature policy and / or commitment type is used with regards to the signature that will be created, it will be displayed to the user.

If the signature was created based on a specific signature policy, the AdES signature will contain a reference to the signature policy. Currently the only signature policy supported is the itsme® Generic Signature Policy for qualified electronic signatures with OID 1.3.6.1.4.1.49274.1.1.7.

The Connective SCA support PAdES and XAdES signature formats compatible with The AdES created by the SCA will include the certificate chain.

The signature created will be provided to the signer via a mail containing a download link or via the Connective eSigning portal.

In order to have timestamping redundancy, double timestamping is implemented for signatures created with itsme Sign. Following TSAs are used:

- *Primary: Certigna (or Camerfirma for some instances in Spain) with backup globalSign*
- *Secondary (only in case of itsme Sign): Quovadis with backup belgium TSA*

The SCA supports XAdES (ETSI EN 319 132 part 1-2 version 1.1.1), CAdES (ETSI EN 319 122 part 1-2 version 1.1.1), PAdES (ETSI EN 319 142 part 1-2 version 1.1.1) and ASiC (ETSI EN 319 162 part 1-2 version 1.1.1).

The following signature classes are supported when the signature creation is requested by a DA: BASELINE-B, BASELINE-T, BASELINE-LT and BASELINE-LTA

PROOF OF ORIGIN SIGNATURE

In order to proof the origin and integrity of this document, it is signed by Nicolas Metivier (CEO of Connective)

Digitally signed by Nicolas Metivier
Date: 14/04/2021 11:05:16