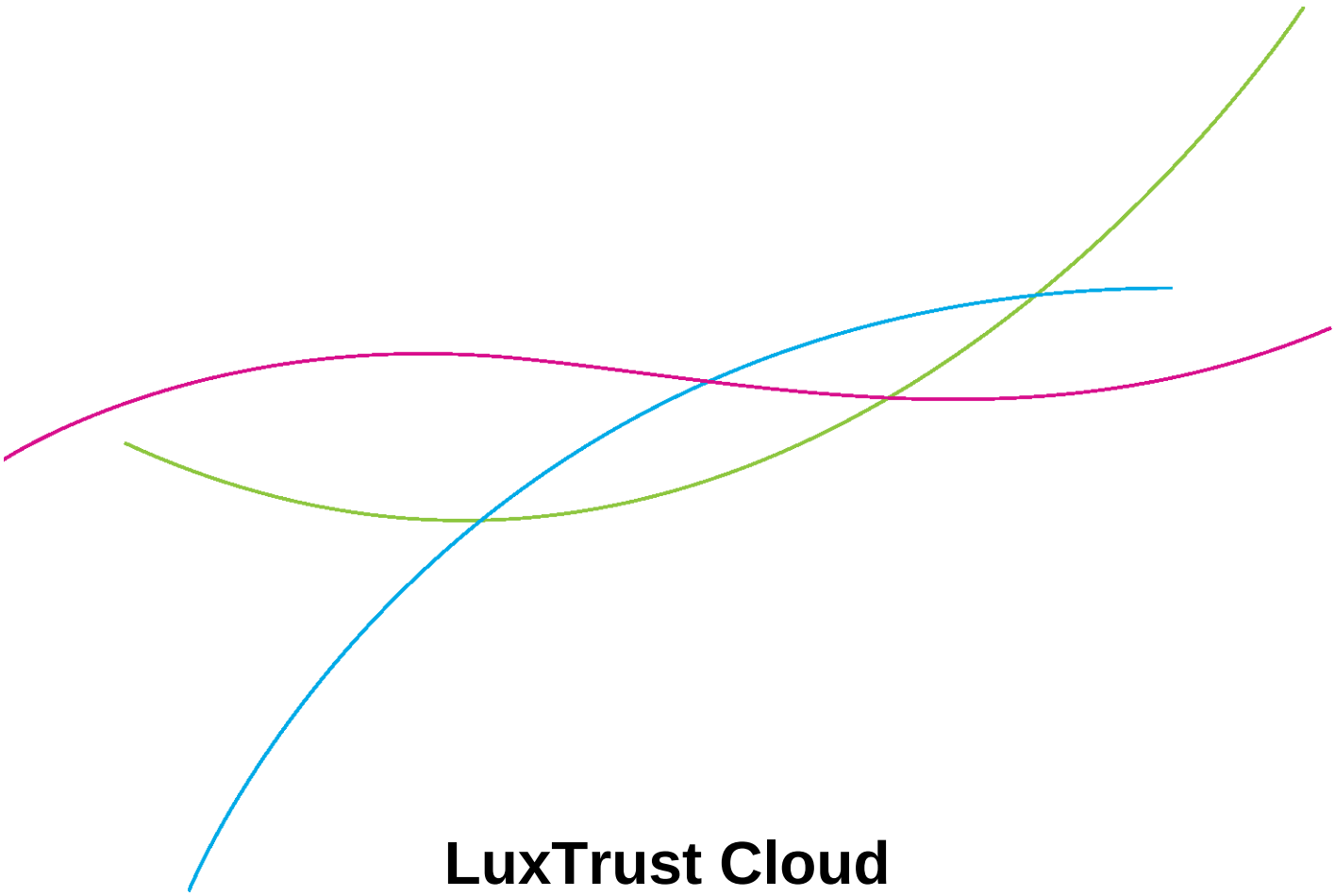


LuxTrust Cloud Validation CPS

Document reference:
1.3.171.1.4.0.1.0.1.0

Date issued:
2020-07-28

Version: 1.1

LuxTrust S.A
IVY Building | 13-15, Parc d'activités | L-8308 Capellen
Luxembourg | VAT LU 20976985 | RCS B112233
Business Number N°00135240/0
Phone: +352 26 68 15 – 1
Fax: +352 26 68 15 – 789

Revision History

Version	Date	Description of Change
1.0	08/04/2020	First version
1.1	28/07/202	Typo correction

Intellectual Property Rights

Disclaimer

In case of discrepancy in interpretation concerning a given linguistic version with respect to the English reference version, the English version shall prevail.

References

[1] Regulation 910/2014/EU – Electronic identification and trust services for the electronic market, August 2014

[2] ETSI EN 319 102-1 – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, May 2016

[3] ETSI TS 119 102-1 – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, August 2018

[4] ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

[5] ETSI TS 119 441 – Policy requirements for signature validation services operated by a TSP

[6] ETSI EN 319 401 : General Policy Requirements for Trust Service Providers

[7] LuxTrust Cloud Validation Policies

CONTENTS

1. Introduction

This document describes what practices are in place for the provisioning of the default LuxTrust Signature Validation Service (LSVS).

The document is structured as described by the ETSI standard TS 119 441 Annex A

1.1. Overview

1.1.1. TSP IDENTIFICATION

The service provider is LuxTrust S.A and is identified with a registered object identifier (OID): 1.3.171.1

1.1.2. SUPPORTED VALIDATION SERVICE POLICY (IES)

The supported signatures validation policies are documented in the LuxTrust Cloud Validation Policies document.

The LuxTrust Cloud Validation Policies is available on the LuxTrust website (cf. base URL https://www.luxtrust.lu/en/repository)

1.2. Signature Validation Service Components

1.1.3. SVS ACTORS

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

Signature validation protocol (SVP): set of rules and guidelines for communicating data with the purpose of validating signatures

Signature validation client (SVC): component or piece of software that implements the signature validation protocol on the user's side

Signature validation service server (SVSServ): component that implements the signature validation protocol and processes the signature validation on the SVSP's side

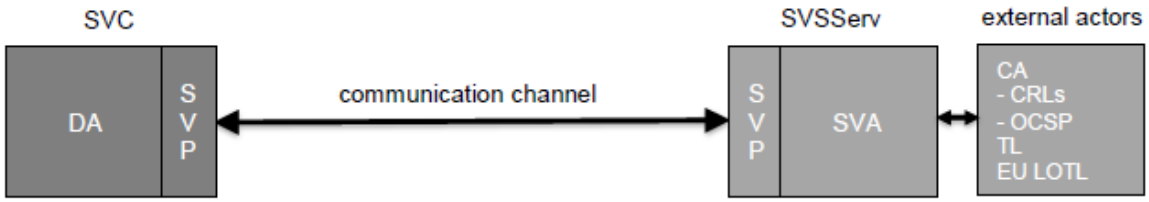
User: application or a human being interacting with an application on top of the signature validation client that requests signature validation

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

1.1.4. SERVICE ARCHITECTURE

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



SVC:

- executes the SVP on the user's side
- builds the signature validation request
- 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 validation report

SVSServ:

- executes the SVP and processes the signature validation on the SVSP side
- runs the SVA that:
  - implements the validation algorithm also defined in ETSI TS 119 102-1
  - can call external actors to fulfil its purpose
- creates the SVR related to the request
- builds the signature validation response

The communication channel between the SVC and the SVSServ transports the signature validation requests and the response. The SVS requires TLS client authentication in order to establish a mutually authenticated communication channel for protecting integrity, authenticity and confidentiality of requests and responses.

1.3. Definitions and Abbreviations

1.1.5. 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.

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

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: process of verifying and confirming that a digital signature is technically valid according to applicable standards and policy constraints

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

Subscriber: legal or natural person bound by agreement with LuxTrust to any subscriber obligations. In the LuxTrust ecosystem, subscribers consist as well from customers (service providers) that have signed a contract with LuxTrust 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 33

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

1.1.6. ABBREVIATIONS

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
ETSI	European Telecommunications Standards Institute
FW	Firewall
LOTL	List Of Trusted Lists
LSVS	LuxTrust Signature Validation Service
MTLS	Mutual TLS authentication
OCSP	Online Certificate Status Protocol
OID	Object Identifier
POE	Proof Of Existence
QES	Qualified Electronic Signature
SCA	Signature Creation Application
SD	Signed Document
SVA	Signature Validation Application
SVC	Signature Validation Client
SVP	Signature Validation Protocol
SVR	Signature Validation Report
SVS	Signature Validation Service
SVSServ	Signature Validation Service Server
SVSP	Signature Validation Service Provider

SYSLOG	System log
TL	Trusted List
TLS	Transport Layer Security
TSP	Trust Service Provider
XML	eXtensible Markup Language
WAF	Web Application Firewall

1.4. Policies and practices

1.1.7. ORGANIZATION ADMINISTRATING THE TSP DOCUMENTATION

The Organisation administering the CPS is LuxTrust S.A. acting as Certification Service Provider (CSP) via its LuxTrust CSP Board, acting as Policy Approval Authority.

The CSP Board, acting as Policy Approval Authority, is composed of the senior management of LuxTrust S.A. The procedure used to add or remove members of the CSP Board is determined and ruled by internal documents.

LuxTrust contact information	
Postal Address	LuxTrust S.A. IVY Building 13-15, Parc d'Activités L-8308 Capellen
E-mail address	cspboard@luxtrust.lu
Website	www.luxtrust.lu

Prior to becoming applicable, modifications to the CPS are announced in the repository as available on https://repository.luxtrust.lu.

1.1.8. CONTACT PERSON

For specific questions concerning the present policy document, please use the following email address or telephone number:

Email: questions@luxtrust.lu

Phone: +352 24 550 550.

1.1.9. TSP (PUBLIC) DOCUMENTATION APPLICABILITY

The CPS and the LuxTrust Cloud Validation Policies are available on the LuxTrust website (cf. base URL https://www.luxtrust.lu/en/repository)

The procedure to become acknowledged as a Subscriber, including the The Terms and Conditions applicable to the Validation Service, and the pricelist describing the related charging fees can be obtained upon request from questions@luxtrust.lu.

2. 2. Trust Service management and operation

1.5. Internal organization

2.1.1. ORGANIZATION RELIABILITY

2.1.1.1. LUXTRUST'S OBLIGATIONS

LuxTrust offers its Trust Services under non-discriminatory practices.

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

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

LuxTrust fulfils general security requirements set out in article 19 of the eIDAS Regulation as further developed in ETSI EN 319 401.

In relation to the validation Trust Services, LuxTrust provides validation of (Qualified) Electronic Signatures and Seals in accordance with article 33 of the eIDAS Regulation and relevant sections of ETSI TS 119 102-1 Electronic Signatures and Infrastructures.

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 ILNAS the Luxemburgish national Supervisory Body.

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 ensure the security and maintain the confidentiality of applicable credentials to use the Validation Services and promptly communicate LuxTrust any circumstance raising suspicion or risk of them being compromised.

2.1.1.3. OBLIGATIONS OF ALL EXTERNAL ORGANIZATIONS

Any external service provider and providing support to the LuxTrust Signature validation service (data centre hosting, ...) is located in Luxembourg and is responsible for ensuring business continuity, as well as physical security and monitoring systems alerting LuxTrust of any attempt to gain unauthorised access to its perimeter.

LuxTrust regularly monitors the implementation of the applicable controls.

All these external service providers implement practices, procedures and controls that comply with the requirements expressed in this LuxTrust's CPS.

These provider are subject to regular audits by LuxTrust and must ensure that they comply with the eIDAS requirements applicable to them

2.1.1.4. LUXTRUST'S LIABILITY

In accordance with Article 13 of the eIDAS Regulation, LuxTrust S.A. will only be liable in relation to the LuxTrust qualified validation service for damages caused intentionally or negligently due to a failure to comply with its obligations under the eIDAS Regulation. Please refer to the CGV for more details

2.1.1.5. DISPUTE RESOLUTION

The CPS shall be governed by, and construed in conformity with, the laws of the Grand Duchy of Luxembourg.

Prior to litigation, the resolution of complaints and disputes received from customers or other parties about the provisioning of electronic trust services or any other related matters is ruled by the "LuxTrust Dispute Resolution Procedure" as publicly available from https://repository.luxtrust.lu.

The courts of the judicial district of Luxembourg-city have exclusive competence for any dispute arising from, or in connection with, the CPS.

2.1.1.6. CONFIDENTIALITY

The LuxTrust Signature validation service guarantees the confidentiality of an SD according to applicable European and national laws on privacy and Luxembourg laws regarding the financial sector. LuxTrust S.A. particularly and immediately erases all copies of a received SD, if any, from its servers after having performed a requested transaction.

2.1.2. SEGREGATION OF DUTIES

The LuxTrust definition of Roles and Responsibilities as defined by the Organisation Chart specifies the requirements for segregation of duties across these roles.

Please refer to 2.2. Human resources for more details

1.6. Human resources

All members of the personnel staff that involved for the provision of the LuxTrust services are either employees of LuxTrust S.A. or authorised and qualified personnel of sub-contracting entities providing sub-contracted certification and/or time stamping component services.

All members are subject to personnel and management practices that LuxTrust S.A. follows to provide reasonable assurance of the trustworthiness and competence of the staff members within the fields of electronic signature-related technologies and related services.

LuxTrust S.A. acting as CSP obtains a signed statement from each member of the staff on not having conflicting interests with the CSP, on the preservation of confidentiality and the protection of personal data.

LuxTrust S.A. acting as CSP ensures that:

- All tasks, roles and responsibilities with respect to the LuxTrust trusted services are:
    - Described in job descriptions and made available to the concerned personnel. These job descriptions are defined from the view point of segregation of duties and least privileges, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.
    - Allocated to the system of the CSP and/or to the member of the staff according to its trusted role.

- All actions with respect to the LuxTrust trusted services can be attributed to the system of the CSP and/or to the member of the staff that has performed the action.
- Personnel shall exercise administrative and management procedures and processes that are in line with the LuxTrust information security management procedures.
- Trusted or management roles are formally appointed to trusted roles by senior management responsible for security and are not appointed to any person who is known to have a conviction for a serious crime or other offense which affects his/her suitability for the position and/or until necessary checks are completed.
- Managerial personnel possess expertise in the field of electronic signature and related services, in risk assessment and information security as well as possess familiarity with security procedures for personnel with security responsibilities.

1.7. Asset management

LuxTrust S.A., acting as CSP, ensures implementation and maintains appropriate level of protection to its assets and information systems. For this purpose LuxTrust S.A. maintains an inventory of all information assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

1.8. Access control

The LuxTrust's system access is limited to authorized individuals.

In particular:

- Controls (e.g. firewalls) protect the internal network domains from unauthorized access including access by subscribers and third parties.
- Firewalls are configured to prevent all protocols and accesses not required for the operation of the TSP.
- LuxTrust administer user access of operators, administrators and system auditors.
- The administration includes user account management and timely modification or removal of access.
- Access to information and application system functions is restricted in accordance with the information security policy.
- The LuxTrust’s system provides sufficient computer security controls. For this purpose, the administration and security management functions are separated. Particularly, use of system utility programs is restricted and controlled.
- LuxTrust's personnel is identified and authenticated before using critical applications related to the service.
- LuxTrust's personnel shall be accountable for their activities. For this purpose, the event logs are monitored and retained
- Sensitive data are protected against being revealed through storage and restriction of access thereto for unauthorized users.

.

1.9. Cryptographic controls

LuxTrust applies the requirements for cryptographic controls specified in clause 7.5 of ETSI EN 319 401.

The private key of the LuxTrust Signature validation service for signing the validation report is stored and used in a cryptographic module with level of security FIPS 140-2 level 3 or higher, or, respectively, CC EAL4+ oh higher

1.10. Physical and environmental security

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

1.11. Operational security

The operational procedures and responsibilities are defined by the LuxTrust Operating Model based on the ITIL Version 3: support (first line, second line, and third line), request fulfilment, incident management, problem management, change management, release and deployment management, and service asset and configuration management.

Instantiated for specific provisions, the Security and Architecture guidelines provide the policy principles for: separation of the different environments, overall protection from malware and information backup procedures.

This includes event logging, protection of log information, administrator and operator logs, clock synchronization, as well as control of operational software, via the installation of software on operational systems.

The datacenter provides 24/7 monitoring on the infrastructure, network and security components as part of their service offering. LuxTust provides a monitoring for systems (infrastructure as well as application level). LuxTrust collects all technical logging (FW, WAF, Syslog), which provides log collection, log normalization, log correlation and querying capabilities. Based on specific queries and correlations, alerts are triggered to investigate for possible suspicious connections. LuxTrust collects, and protects, all functional logs centrally as the main source for fraud investigations. Together, this allows LuxTrust to configure triggers for activity and alerts.

Operational Logs are kept online at least for 1 year (excluding further archiving, extending this retention period). Transaction logs and signature validation reports have a retention period of 10 years based on legal obligations for archiving and for providing proof in case of disputes. The signature validation report contains all data that was used during the validation (signature itself, revocation data, timestamps, certificates, etc.) but not the signer’s document.

1.12. Network security

LuxTrust S.A. acting as CSP ensures that network security controls (including but not limited to firewalls, network intrusion detection secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc.) are implemented in compliance with the standard ETSI EN 319 401 when this standard impose higher requirements on certification practices.

Detailed descriptions of implemented network security controls are available as internal document(s).

1.13. Incident management

The management of security incidents and improvements is integrated within the overall operations model and the standard incident management procedures there. Incidents are logged into the Service Desk tooling, and assigned based on their classification. Security and privacy incidents are also forwarded to the CISO or DPO respectively, to keep him/her informed, and take immediate appropriate action.

1.14. Collection of evidence

LuxTrust maintains records concerning the operation of the services in scope for the purposes of providing evidence of the correct operation of these 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 protected and backed up to avoid information loss or compromise. Log backups are retained for a minimum period of 10 years.

1.15. Business continuity management

LuxTrust S.A. acting as CSP establishes the necessary measures to ensure full and highly automated recovery of the LuxTrust certification and time stamping services in case of a disaster, corrupted servers, software or data. Any such measures are compliant against the ISO/IEC 27002 standard.

A Business Continuity Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

1.16. TSP termination and termination plans

LuxTrust has created a termination plan that deals with termination notification, subcontractor's management, information maintenance, private key destruction, termination phasing and updating of the termination plan procedure. LuxTrust has taken measure to ensure that the execution of the termination plan is executed in case of bankruptcy.

1.17. Compliance

The CPS and provision of LuxTrust PKI Services are compliant to relevant and applicable laws of Grand Duchy of Luxembourg. LuxTrust employs personnel with the required legal skills and has that fulfil the required roles (e.g. DPO) in order to guard the correct implementation of legal requirements.

LuxTrust is in progress to obtain the Qualified status for its LuxTrust Signature Validation Service and is in this regards under supervision of the Luxemburgish national supervisory body.

3. Signature validation service design

1.18. 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, 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 support the validation policies in accordance with one of validation policies specified in the LuxTrust Cloud Validation Policies document. In addition, an application provider (APP) can define a custom validation policy that must be derived from a policy specified LuxTrust Cloud Validation Policies document and agreed to with LuxTrust when concluding a service contract. In that case, the service configuration for the given APP will apply the rules of the agreed derived policy.

The validation process follows EN 319 102-1 amended by TS 119 102-1.

The validation report is is formatted as a machine- and human-processable XML document and sealed by LuxTrust with an advanced or qualified electronic seal for proving its authenticity and integrity

3.1.2. EU TRUSTED LISTS OF CERTIFICATION SERVICE PROVIDERS

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).

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, each TL can be processed. If they are valid, the service providers and its certificates can be trusted.

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".

1.19. Signature validation protocol requirements

The signature validation protocol will be as follows:

- the SVC sends the SD containing the digital signature(s) to be validated to the SVS
- the SVS sends the signature validation response containing the SVR to the SVC

1.20. Interfaces

3.1.3. 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.

3.1.4. SVSP - OTHER TSP

Communication between the SVSP and other TSPs depend upon the interface that is defined and the 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.

1.21. Signature validation report requirements

The validation process follows EN 319 102-1 amended by TS 119 102-1.

The service issue a signature validation report formatted as a machine- and human-processable XML document and sealed by LuxTrust with an advanced or qualified electronic seal for proving its authenticity and integrity

This validation report is 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 validation report can contain the status indication per validated signature, being:

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

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

The validation report does 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.

The signed attributes are listed in the validation report, however they might be listed in different places.

Some signed attributes are listed by referring to the usual name, but for the ones only acknowledged by the validation service, they are recognized by using an OID or URI indicator.