UAB "NEVDA" OPERATIONAL REGULATIONS FOR QUALIFIED SERVICES

version 1.5

(OID) - 1.3.6.1.4.1.57583.1.1

Valid from 4 July 2022

Table of Contents

1. Introduction

The core activity of UAB Nevda is the development, installation and maintenance of information systems for public sector organizations and business companies.

In 2021, UAB Nevda established the NEVDA Qualified Service Centre (hereinafter - QSC) to provide qualified trust services.

1.1 Overview

This document details the activities of UAB Nevda and QSC in providing Qualified Trust Services.

List of qualified trust services:

1) (**QVal for QESig**) Qualified validation services for qualified electronic signature.
2) (**QVal for QESeal**) Qualified validation services for qualified electronic seal.

1.2 Document amendments and approval

Document preparation timeline:

Version	Date	Description
1.1	14 April 2021	An initial version of the document was prepared
1.2	20 May 2021	The updated version was assigned for review and analysis
1.3	8 September 2021	Version was assigned for audit review
1.4	10 September 2021	After the audit notes, the version was assigned for RRT
1.5	4 July 2022	Final version after RRT approval

Approval of the latest version of the document

Version	Date	Approved by
1.5	4 July 2022	UAB “Nevda“ director deputy Paulius Jonikas

1.3 Terms and definitions, abbreviations

Abbreviations	Description
QVal for QESig	Qualified validation service for qualified electronic signature
QVal for QESeal	Qualified validation service for qualified electronic seal
Qualified services	QVal for QESig and QVal for QESeal service
Elpako	UAB Nevda-managed information system for providing Qualified Services
NEVDA	UAB Nevda
QSC	The business unit of UAB Nevda responsible for the provision of Qualified Services
QSC operational regulations	This document describes QSC's activities in providing Qualified Services
Client	A legal or natural person has signed an agreement with UAB Nevda on the provision of Qualified Services
TSL	Trusted Services List
Time stamp	Data in electronic form, linking other data in electronic form to a specific time and thus creating evidence that the latter existed at that time
Electronic signature	Data in electronic form which are connected or logically linked to other data in electronic form and which the signatory uses when signing
Electronic seal	Data in electronic form connected or logically linked to other data in electronic form to ensure their origin and integrity
Qualified electronic signature	Advanced electronic signature created using a qualified electronic signature creation device and validated with a qualified electronic signature certificate
Qualified electronic seal	Advanced electronic seal developed using a qualified electronic seal creation device and certified by a qualified electronic seal certificate
Time-Stamping Authority	TSA – Time-Stamping Authority, provider of time-stamping services

Signatory	Legally capable natural person who creates the electronic signature
Seal creator	Legal entity that creates that electronic signature
Data security regulations	UAB NEVDA INFORMATION SYSTEM DATA SECURITY REGULATIONS
User administration rules	UAB NEVDA INFORMATION SYSTEM USER ADMINISTRATION RULES
Information processing rules	UAB NEVDA INFORMATION SYSTEM SAFE ELECTRONIC INFORMATION PROCESSING RULES
Operation continuity plan	UAB NEVDA INFORMATION SYSTEM OPERATION CONTINUITY MANAGEMENT PLAN
Incident management rules	UAB NEVDA INFORMATION SECURITY INCIDENT MANAGEMENT RULES
eIDAS	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
Qualified electronic signature creation device	An electronic signature creation device that meets the requirements set out in Annex II of the eIDAS Regulation
Certificate of qualified electronic signature	Electronic signature certificate issued by a qualified trust service provider and meeting the requirements set out in Annex I of the eIDAS Regulation
ETSI	European Telecommunication Standardisation Institute
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
OCSP	Online Certificate Status Protocol. Certificate validation compliant with RFC 6960 recommendations
CRL	Certificate revocation list. Certificate validation compliant with RFC 5280 recommendations
Repository	QSC information database, available to users online at any time at www.elpako.eu

Other terms and abbreviations used in this document have the meanings ascribed to them in 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

1.4 Identification

QSC operational regulations are published at the Repository.

QSC operational regulations OID - 1.3.6.1.4.1.57583.1.1

Name	Value
ISO	1
ISO-recognized organization	3
U.S. Department of Defense	6
Internet	1
Private company	4
IANA registered private company	1
UAB Nevda	57583
UAB Nevda division QSC	1
QSC operational regulations document	1

1.5 List of documents used

The creation of qualified services and the provision of services are based on the following documents:

- latest version of 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 (hereinafter referred to as eIDAS);

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as - General Data Protection Regulation);
- latest version of the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions;
- resolution of the Republic of Lithuania No 144 of 18 February 2016 "Regarding the appointment of the trust service supervision authority and the body responsible for compiling, maintaining and publishing a national trusted list";
- The latest version of the Law of the Republic of Lithuania on the Legal Protection of Personal Data;
- order of the director of the Communications Regulatory Authority of the Republic of Lithuania No 1V-588 of 21 June 2018 "On the approval of the specification of the procedure for granting status of qualified trust service providers and qualified trust services and incorporation thereof in the national trusted list and provision of activity reports of qualified trust service providers";
- order of the director of the Communications Regulatory Authority of the Republic of Lithuania No 1V-594 of 4 June 2019 "On the approval of the description of the procedure for reporting on violations of the security and/or integrity of trust services";
- ETSI EN 319 403 v2.3.1: Requirements for conformity assessment bodies assessing Trust Service Providers;
- ETSI EN 319 401 v2.3.0: General Policy Requirements for Trust Service Providers;

1.6 Organization issuing and processing QSC operational regulations

UAB Nevda

Company code: 121931451

Address: Savanorių av. 178F 03154 Vilnius

Website: www.nevda.lt

Email: info@nevda.lt

1.7 Contact persons

Information on all issues related to this document and qualified services is provided by UAB Nevda QSC division.

Contact us by email: eidas@elpako.eu

1.8 Information about Qualified Services

Information on qualified services is available at www.elpako.eu/teisine-informacija.

Information on the services provided is reviewed from time to time and updated at least once a year.

Nevda guarantees the availability of the Repository 99.99% of the time.

2. General provisions

2.1 Liability

NEVDA assumes liability for losses incurred by users in accordance with the procedure established in Art. 13 of eIDAS and the Law of the Republic of Lithuania on Electronic Identification and Trust Services.

The liability of qualified service providers is established in the latest version of eIDAS, regulatory enactments of the Republic of Lithuania regulating trust services insofar as they do not contradict eIDAS, and the concluded agreements.

2.1.1 Liability of activity

NEVDA is responsible for the quality and availability of the provided services, but only within the limits of the operation of the system it manages.

NEVDA is not responsible for systemic failures of third parties, disturbances (fixed outside the scope of NEVDA's operation), due to which the provision, quality and availability of services may be disrupted.

NEVDA shall not be liable for any failures or disturbances in the Customer's systems that may have disrupted the provision, quality and availability of the provided services.

NEVDA assumes liability for losses incurred by users in accordance with Article 13 of eIDAS. and in accordance with the procedure established by the Law on Electronic Identification and Trust Services of the Republic of Lithuania.

2.1.2 Financial liability

In order to ensure financial liability obligations, Nevda ensures its activities by at least the amount fixed in Article 10 of the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions.

2.2 Legal provisions and interpretation

2.2.1 Legal force of qualified electronic signature and seal

- A qualified electronic signature has the same legal force as a written signature. A qualified electronic signature attested by a qualified certificate issued in one Member State shall be recognized as a qualified electronic signature in all other Member States;
- A qualified electronic seal is subject to a presumption as to the integrity of the data to which the qualified electronic seal is linked and the appropriateness of the origin of that data. A qualified electronic seal attested by a qualified certificate issued in one Member State shall be recognized as a qualified electronic seal in all other Member States.

2.2.2 Key legislation

The rights and responsibilities of the participants of the Qualified Services, the requirements for the Qualified Service Providers and their liability are established in the regulatory enactments specified in sub--article 1.5 of this document.

2.2.3 Dispute resolution procedure

Any disputes between NEVDA and the Clients shall be settled through negotiations. If the dispute is not resolved through negotiations, it shall be resolved in court in accordance with the applicable legislation of the Republic of Lithuania

2.3 Fees of qualified services

Fees for the provision of qualified services are published at https://www.elpako.eu/teisine-informacija.

2.4 Customer service procedures

- Customer may submit questions, concerns or complaints regarding the Terms of Service for Qualified Services to our customer service team via email support@elpako.eu or on the website https://elpako.eu/kontaktai/ in the inquiry form. We will respond to the customer's request no later than within 5 calendar days.
- Customer who is dissatisfied with the quality of the Qualified Services provided may additionally submit a complaint to the Communications Regulatory Authority of the Republic of Lithuania by e-mail. by e-mail rrt@rrt.lt (website https://www.rrt.lt), or by e-mail to the State Consumer Rights Protection Service. email tarnyba@vvtat.lt

2.5 Provision of information

2.5.1 Provision of information to supervisory authority

- Not later than within 3 business days Nevda informs the supervisory authority of any changes in the provision of its Qualified Trust Services that may affect the quality of the provision of Qualified Services;
- Not later than 3 business days in advance informs the recipients of the trust services and the Supervisory Authority about the planned works, during the performance of which there is a probability of disruption of the uninterrupted provision of the Qualified Services;
- By February 1st each year, submits to the Supervisory Authority a report on the activities of the previous calendar year, which shall indicate the total number of qualified electronic signatures and qualified electronic seals verified during the previous calendar year.

2.5.2 Public information of Nevda

NEVDA's publicly available information includes:

- information on the status of the provision of Qualified Services;
- Terms for the creation and management of qualified services;

- Price lists for qualified services;
- User instructions;
- Summaries of inspection reports of Nevda's activities prepared by the authorized bodies;
- Other miscellaneous information of organizational kind or proving reliable performance which relates to the provision of Qualified Services:
    - Findings of the independent audit of NEVDA's activities;
    - Various advertisements related to the Qualified Services provided.

2.5.3 Information update rate

The information provided by NEVDA shall be updated at the following intervals or frequencies:

- Changes are made, approved and published in accordance with the Data Security Regulations;
- Other information to be published and updated (e.g. Nevda performance audit findings, etc.) is published upon receipt or preparation within a reasonable time

2.6 Conformity verification

Conformity of NEVDA's activities for the proper provision of Qualified Services shall be verified:

- in accordance with Art. 20 (1) of eIDAS, NEVDA shall be audited at least every 24 (twenty-four) months by a conformity assessment body;
- in accordance with Art. 20 (2) of eIDAS, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of NEVDA, at the expense of NEVDA, to confirm that the qualified trust services provided fulfil the requirements laid down in this eIDAS;
- in accordance with Art. 20 (3) of eIDAS, where the supervisory body requires NEVDA to remedy any failure to fulfil requirements under eIDAS and where NEVDA does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of NEVDA or of the affected service it provides and inform the body referred to in Article 22 (3) for the purposes of updating the trusted lists;

2.7 Confidentiality

2.7.1 Personal data

- NEVDA must process personal data in accordance with the General Regulation on the Protection of Personal Data and the Law of the Republic of Lithuania on the Legal Protection of Personal Data, which implements the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in so far as it is not contrary to the General Regulation on the Protection of Personal Data. Personal data are kept for an appropriate, necessary period (including in the event of termination of NEVDA activities), but not longer than needed for the purposes of the processing, which shall be communicated to the

person for use in legal proceedings and thus ensure activity continuity;
- when personal data are no longer needed for the purposes of their processing, they are destroyed, except for those data that must be transferred to state archives in cases prescribed by law.

2.7.2 Classified information

Classified information that is stored and processed in accordance with Nevda's internal regulations is:

- log files
- records of disruptions in the provision of trust services, if their publication may endanger the provision of Qualified Services;
- records of internal and external inspections of NEVDA's activities, if their publication may endanger the security of NEVDA's services;
- contingency plans;
- Information about how to protect hardware and software and perform trust service operations.

2.7.3 Non-classified information

- Terms for the creation and management of qualified services;
- Price lists for qualified services;
- User instructions;
- Summaries of Nevda activity inspection reports prepared by authorized bodies.

2.7.4 Protection of information

- In order to protect stored records from theft or falsification, Nevda takes preventive measures related to the proper and effective control of the physical, technical, procedural security and reliability of personnel;
- The records are stored in trusted systems so that they may be authenticated and the records and changes can only be made by persons authorized by Nevda.

2.7.5 Provision of information to law enforcement

Classified information of Nevda may be provided to law enforcement officials only in accordance with the requirements of the regulatory enactments of the Republic of Lithuania.

3. Requirements for Qualified Services

This section defines the requirements for Nevda's activities in providing qualified services.

3.1 Requirements for QVal for QESig and QVal for QSeal services

Qualified services are a validation carried out in accordance with the requirements of Article 32, 33 and 40 of eIDAS. Qualified services enable relying parties to obtain the result of the validation procedure in an automated manner that is reliable, efficient and linked to

the qualified validation service provider's advanced electronic signature or advanced electronic seal.

The main requirements for Qualified Services are:

- the certificate confirming the signature was a qualified electronic signature certificate at the time of signing;
- The qualified certificate was issued by a qualified trust service provider and was valid at the time of signing.
- the signature validation data correspond to the data provided to the relying party;
- unique data set identifying the signatory in the certificate is properly provided to the relying party;
- If a pseudonym was used at the time of signing, this is clearly indicated to the relying party.
- The electronic signature is created using a qualified electronic signature creation device;
- The integrity of the signed data has not been compromised;
- The requirements set out in Article 26 of the EIDAS have been complied with at the time of signing;
- The system used for the validation of a qualified electronic signature gives the relying party a correct result of the validation procedure and allows the relying party to identify any security issues.
- Signature verification is performed in accordance with the *ETSI TS 119 102-1* standard;
- The signature verification report is generated in accordance with the *ETSI TS 119 102-2* standard.

3.2 Collection and storage of records about the provision of Qualified Services

3.2.1 Registered events

All qualified service order operations are recorded in a secure operation log. Log entries are stored for at least 10 years. Fixed service order operations include:

- qualified service type validation;
- time and date;
- unique client identifier;
- unique request identifier;
- logic value or service successfully provided.

An information system component information event log is used to analyse the actions of information systems, their users, and administrators. Recorded data include:

- Information about enabling, disabling, or resetting information system servers, application software and other information system components.
- Infrastructure configuration change actions performed by system administrators;
- Software update actions.

The diagnostic log records detailed system actions that are used to analyse, diagnose, and troubleshoot system performance issues. The main users of the diagnostic log are system developers and administrators. The Error Log records information about system failures and errors, including the time, source, description, and details of the failure.

3.2.2 Records on events review periodicity

The logs of the operations and activities of the NEVDA system are reviewed at least once a month. Any major event or occurrence due to a malfunction of the systems must be described. Electronic information of event system component event logs related to actions performed by information system users and information system administrators are reviewed within the terms and in accordance with the procedure established in the Data Security Regulations.

3.2.3 Record storage period

The NEVDA system operation and activity logs are kept by NEVDA for 10 (ten) years, further storage is regulated by the latest version of the Law of the Republic of Lithuania on Documents and Archives.

3.2.4 Record protection

NEVDA system operation and activity logs are backed up on a daily basis. If the number of records provided for a particular log is exceeded, the contents of the log are transferred to the archive.

3.3 Data archiving

3.3.1 Data transferred to the archive

The following is archived:

- system operation and activity logs;

3.3.2 Period of storage of data in the archive

Data is stored in the archive for 10 (ten) years, further storage is regulated by the Law of the Republic of Lithuania on Documents and Archives.

3.3.3 Making of backup copies

Backups enable the system to restore after a failure. Copies of the following software and data files are made for this purpose:

- installation disk with Elpako system software;
- Logs of operations and activities of Elpako systems.

3.4 Security incidents and their management

Incidents are classified and managed according to Nevda-approved documents:

- incident classification is described in the Incident Management Document;
- The management of critical security incidents is described in the Activity Continuity Plan.

3.4.1 Incident registration, identification and analysis procedure

NEVDA follows this procedure:

- Upon recording of information system malfunctions / incidents that indicate unusual or inconsistent operation of information system components, such malfunctions / incidents shall in all cases be recorded in a logbook that shall be archived and protected from tampering, loss, unauthorized or unintentional alteration or destruction to ensure that evidence of criminal offenses committed during electronic information security (cyber) incidents be adequate and sufficient for law enforcement authorities to establish the fact of criminal offenses and that those who have committed criminal offenses cannot deny it;
- Once a malfunction / incident is registered, they are prioritized and identified. During identification, the event record is recognized and assigned a category and priority, depending on the settings of the specialized event log analysis tools;
- The analysis assesses whether the event or set of events at a given point in time complies with certain alert generation rules set by specialized event log analysis tools. If, during the analysis, specialized event log analysis tools determine that a particular event or set of events at a given time meets certain established alert generation rules, the specialized event log analysis tools automatically generate an alert;
- Administrators of information system components must review the generated alert and, if necessary, inform the responsible persons about the alert, its content and circumstances;
- The designated information security officer must review the generated alert and assess whether it may be related to breaches of security and integrity under Article 19 (2) of eIDAS. If it is established that the incident may be related breaches of security and integrity under Article 19 (2) of eIDAS, the security officer immediately, but not later than within 4 (four) hours, convenes the working group provided for in the Activity Continuity Plan. The Supervisory Authority and natural or legal persons are informed about the said incidents in accordance with the procedure described in the Incident Management Document no later than within 24 (twenty-four) hours;
- Must record the relevant incident, marking it as related to breach of security and integrity provided for in Art. 19 (2) of eIDAS;
- Informs the supervisory authority no later than within 3 business days from the control or termination of the registered breach, which had a significant impact, by submitting a notification according to the prescribed form.

3.5 Termination of trust services

Before terminating the provision of Qualified Services, Nevda undertakes to act in accordance with a termination plan agreed with the Supervisory Authority (hereinafter - "the agreed plan"), including the following actions (to the extent that they are not contrary to the agreed plan):

- all related persons and organizations, as well as the supervisory authority, must be informed about the termination of the Qualified Services not later than 3 (three) months before the planned termination of the Qualified Services;
- taking into account the expected date of termination of services, but not later than 2 (two) months in advance, submits to the supervisory authority:
  - information on the activity successor;
  - activity adoption agreement;
  - detailed plan for the termination of the provision of Qualified Services.

- If upon deciding to terminate the provision of Qualified Services, the activity is not transferred to a third party, Nevda must ensure the preservation of the activity records.

3.6 Solutions and services used by third parties

Nevda, by using third party solutions or services, always inspects and ensures that the technical and organizational means used by third parties to ensure the quality of service and information security are at least equivalent to the minimum level of information security required by Nevda.

Qualified Services use the solutions and services offered by Microsoft Azure

Who	Physical location	Security assurance
Production application	Microsoft Azure Data Centre, Northern European region. PaaS service “App service“	Microsoft-managed data centres meet all modern security standards (https://docs.microsoft.com/en-us/azure/compliance). Access rights are limited.
Production database	Microsoft Azure Data Centre, Northern European region. Microsoft SQL Server	Microsoft-managed data centres meet all modern security standards (https://docs.microsoft.com/en-us/azure/compliance). Access rights are limited. The firewall restricts access only from the product application and from the internal network of UAB Nevda.
UAB Nevda advanced seal	Microsoft Azure Data Centre, Northern European region. Azure KeyVault key storage service	Microsoft-managed data centres meet all modern security standards (https://docs.microsoft.com/en-us/azure/compliance). All operations with the company stamp certificate held in the Azure KeyVault service are audited. Access is restricted.

3.7 General requirements for qualified service provider

The general requirements for qualified suppliers are described in ETSI EN 319 401.

4. Physical, procedural and personnel security control

4.1 Physical security control

The Elpako information system, operator workstations, and information resources have been installed and are stored in a dedicated location that is physically protected from unauthorized access, destruction, or removal of equipment. Access to key elements of the system is monitored. Every entry of persons into it is registered in the data centre; the stability, of the power supply, the temperature and the humidity are recorded and monitored.

4.1.1 Location

Savanoriu av. 178F, 03154 Vilnius, Lithuania

4.1.2 Physical access

The hardware and software that ensures the provision of qualified services operates in the Data Centre, where physical access is restricted.

4.1.3 Electrical power supply and air conditioning

The hardware and software that ensures the provision of qualified services operates in the Data Centre, which ensures an uninterrupted supply of electrical power and in which air conditioning equipment operates.

4.1.4 Protection from water spills

The hardware and software that ensures the provision of qualified services operates in the Data Centre, which provides protection against water spills.

4.1.5 Fire protection

Hardware and software that ensures the provision of qualified services operates in the Data Centre, where automatic fire extinguishing systems have been installed.

4.1.6 Cryptographic key protection

Qualified services use cryptographic keys stored in a properly protected Microsoft Azure environment.

No copies of cryptographic keys are made.

4.1.7 Storage of data carriers

Depending on the importance of the information, media with archive data and data backups are stored in fireproof safes.

4.1.8 Destruction of carriers

Paper and electronic media containing information affecting the security of the provision of Qualified Services shall be destroyed by special shredding facilities at the end of the storage period of that information.

4.2 Procedural security control

4.2.1 Employee duties

The positions on which QSC's activities depend are:

- Information security officer. General responsibility for the implementation of security policy. The responsibilities and functions of the IT security officer are described in the Data Security Regulations;
- Chief Administrator of Elpako. Responsible for the proper functioning of the Qualified Services. Installs and configures the equipment used; sets system and network parameters;
- Assistant administrator of Elpako. Substitutes the primary administrator of Elpako as needed.

4.2.2 Identification of duties and authentication

The identification and authentication of QSC staff positions is performed in the following ways:

- by compiling a list of persons allowed to enter QSC premises;
- by compiling a list of persons who are allowed physical access to the Elpako system and network resources;

The rules specified in the User Administration Rules ensure that:

- each user of the information system is unique and directly linked to a specific person;
- system login details may not be shared with any other person;
- there are limited functions (arising from the duties of a particular person).

4.3 Personnel reliability control

4.3.1 Qualification requirements

Persons are employed in accordance with the requirements of the Labour Code of the Republic of Lithuania. Recruitment is formalized by an employment contract. The rules of procedure set out the general qualification requirements for staff:

- to speak Lithuanian;
- to have the required education or qualifications;
- to be able to work with computers and other organizational equipment;
- to speak a foreign language (if required).

In addition to the above general requirements, it is guaranteed that the persons performing the duties assigned to the QSC:

- have signed an agreement on the performance of duties and responsibilities;
- have attended internal training relevant to their responsibilities;
- have attended training related to the protection of personal data and confidential information, have read the security documents and have signed a commitment to keep secret confidential information, have read the security documents.
- do not have an outstanding or unexpunged conviction for committing intentional crimes

4.3.2 Requirements for employees

Employees performing contracted assignments (external service providers, software developers, etc.) are inspected according to the same procedures as applicable to QSC staff.

5. Technical implementation

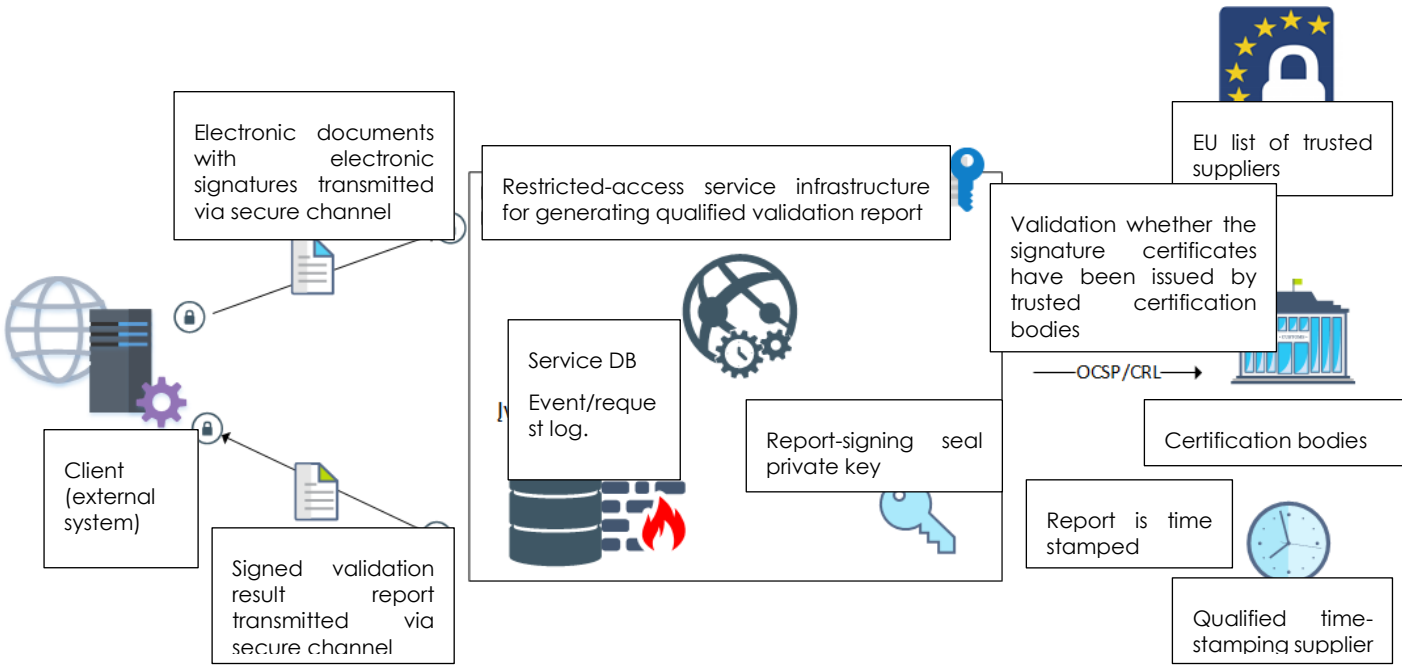
5.1 Implementation of qualified service for signatures/seals

The result of the qualified service is a report on electronic signatures stamped with an advanced electronic seal of UAB Nevda. Qualified Service Reporting Format: XML Report according to the ETSI TS 119 102-2 standard. The report shall be authenticated by an electronic seal.

Elpako software performs validation of electronic signatures prepared in the following formats:

- *EN 319 122* (AdES)
- *EN 319 132* (XAdES)
- *EN 319 142* (PAdES)
- *EN 319 162* (ASiC)

Service operation diagram:



Schematic diagrams of the service operation according to the ETSI TS 119 102-1 standard are given in the diagrams below:

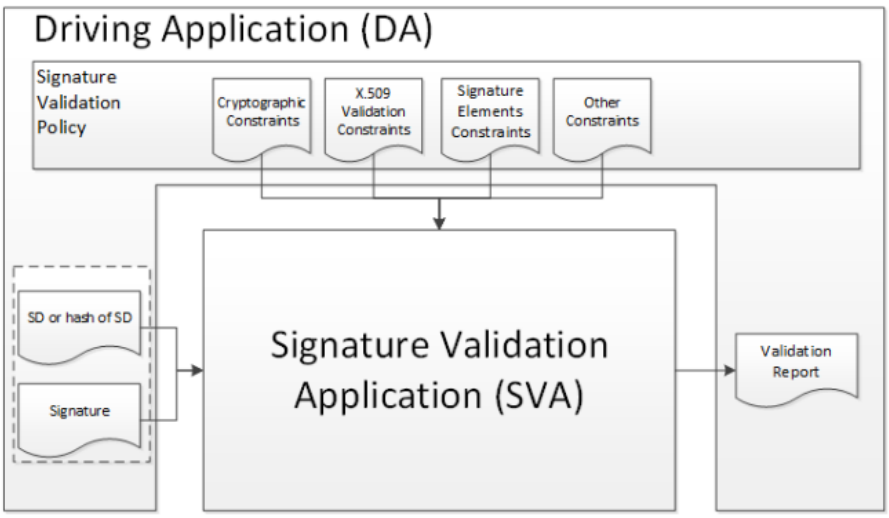


Figure 11: Conceptual Model of Signature Validation

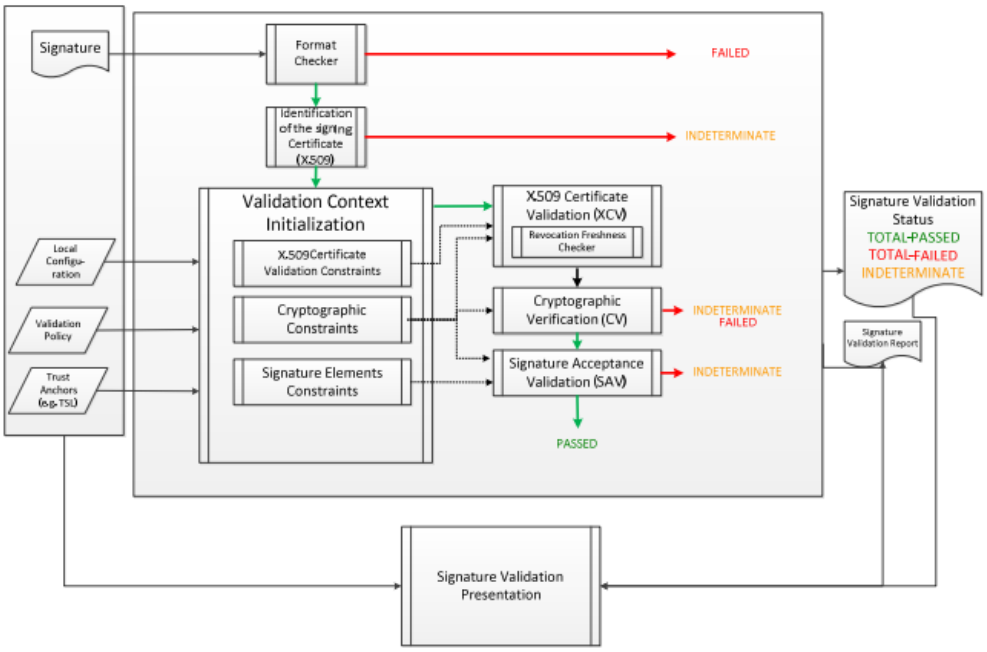


Figure 12: Basic Signature Validation

5.1.1 Qualified service validation process

According to the ETSI EN 319 102-1 standard, after validating an electronic signature, there are three possible signature or stamp validation statuses:

- TOTAL-PASSED: the signature complies with the established validation policy and has passed all validation procedures;
- TOTAL-FAILED: Invalid signature format or failed verification procedures;
- INDETERMINATE: The signature validation was successful, but the information is missing whether the electronic signature is indeed valid.

During each validation process, the detailed information on which basis the signature status was assigned is provided.

The validation process is carried out in accordance with a provided validation policy – it is verified whether electronic signatures are advanced (AdES), whether signatures are validated by qualified certificates (AdES / QC) and whether they fully qualified (QES). All certificates and related certificate chains are validated against the European Union's list of trusted suppliers. This validation also includes the validation of certificates that are signed by the CRL, OCSP, and timestamps.

The validation process policy may be changed with the prior agreement of the required validation elements with the client. In all other cases, the default validation policy is used.

The unique identifier of the default qualified validation policy is identified by the following identifier: 1.3.6.1.4.1.57583.1.1

The procedures described in the ETSI TS 119 172-4 standard are taken into account when validating signature / timestamp certificates. Qualified validation tests are available here.

The validation result is communicated to the client through the Elpako API application program interface. Upon receipt of a document from the client for validation, the Elpako system performs the validation without storing the document. After validation, the result is transformed into human / computer readable XML format and the result is automatically stamped by UAB Nevda. This qualified validation result can then be used for transformation into other forms. Within this qualified service, it is unknown what the client will do with a qualified validation response.

5.1.2 Reliability report authenticity

After verifying the signatures, an XML report is generated according to the ETSI TS 119 102-2 standard. The report is signed with this qualified certificate approved by UAB Nevda advanced seal.

Certificate: **C=LT, O=UAB NEVDA, CN=Elpako QVal**

Certificate-issuing authority: **C=LT, OU=RCSC, O=VI Registru centras - i.k. 124110246, CN=RCSC IssuingCA**

Certificate serial number: **70944e6fb3a36b2e000000049efc**

Certificate SHA-1 cipher (thumbprint): **F2E75D0BD269B2FC99DCDB6229BF7B6639EAF1B8**

5.1.3 Method for providing qualified service

Qualified services are provided through an application program interface (API). Examples of an application program interface request are may be found here.

5.2 General implementation principles for qualified service provision

5.2.1 List of trusted suppliers of the European Union

In order for each country of the European Union to be able to exchange lists of trusted suppliers, the European Commission publishes centrally the places where the lists of trusted suppliers are published throughout the European Union. When synchronizing the trusted supplier lists, the information in those lists is authenticated. The information contained in the trusted supplier lists is used to

determine the qualification of signature, CRL, OCSP and timestamp certificates within the European Union.

5.2.2 Communication channels

A secure encrypted HTTPS TLS channel is always used for communication between the client and the qualified service. This ensures the confidentiality of the data transmitted. All client requests are authenticated according to a key assigned to the client.

Communication between the qualified service and external trusted systems (time stamps, certification centres) is performed according to protocols published by external trusted suppliers.

5.2.3 Authentication

All requests for qualified services are authenticated with the authorization key assigned to the client.

5.3 Data and traffic

Qualified services are provided to the client after authentication. Clients are other systems that are given an authentication key. The client sends an electronic document (data) containing secure signatures / stamps, signature certificates, certificate public keys via a secure HTTPS channel. Further processing of the document according to the selected qualified service is performed (inspection, preparation for long-term storage). To reduce the risk, the document is kept only for the time required to perform a certain qualified service.

During the qualified validation - upon receipt of the document and signatures, it is validated whether the document has not been altered after signing, or whether the parts declared are indeed signed. Signatory certificates are being validated. During these validations, the certificate-issuing body may be contacted to transfer the certificate identification numbers.

During qualified preparation for long-term storage - operations are performed in the same manner as during validation. In addition, the information that may be used for verification in the future is included in the document. Qualified time stamps are put on this information. When placing a time stamp, information encoded by cryptographic hash operations is transmitted to a qualified timestamp provider.

The reliability of the certificates is validated against a pre-synchronized (once a day) pan-European list of trusted suppliers. Validation of the certificate is based on the information contained in the signature certificate concerning the issuing body.

An electronic document and its contents can be absolutely any and we do not know them in advance. During the validation and preparation for long-term storage, cryptographic hash operations are performed automatically with the data to check whether the data has been changed.

Electronic signatures store the information of the signatory's certificate and its public key. The certificate may contain the person's name, surname, position, pseudonym, certificate identification number, personal code, etc. This information is included in the certificates by the issuing body. Each certificate-issuing body records different information, depending on national practices, certificate profiles, and etc.

When the qualified validation report is created, it is signed with the NEVDA advanced electronic seal. The private key for the seal certificate is stored in the restricted-access software. Each case of use of the private key of the electronic seal is recorded and audited.

All transactions and requests (of the Client to the Elpako Information System) are audited and stored in a database according to a client key assigned.