Operational Regulations and Policies for the Provision of Qualified Services

Document version: v1.3

Unique document number ID (OID): 3.6.1.4.1.60536.1.1

Valid from 2024-03-01

Table of Contents

1. INTRODUCTION

The main activity of UAB iSense Technologies is development, implementation and maintenance of information systems for public sector organisations and business companies.

1.1. Overview of the document

This document defines in detail the activities of UAB iSense Technologies in the provision of Qualified Trust Services.

List of qualified trust services:

- (QVal for QESig) Qualified validation service for qualified electronic signatures.
- (QVal for QESeal) Qualified validation service for qualified electronic seals.

1.2. Amendments to the Document

Version	Date	Description
1.1	25/06/2023	Initial version of the document
1.2.2	29/06/2023	Working version of the document
1.3	01/12/2023	Version for coordination with RRT

1.3. Terms and Abbreviations Used

Abbreviations	Description
QVal for QESig	Qualified validation service for qualified electronic signatures
QVal for QESeal	Qualified validation service for qualified electronic seals
Qualified services	QVal for QESig and QVal for QESeal services
ISENSE	UAB iSense Technologies
VERIFFY IS	Information system managed by ISENSE for the provision of qualified services
Documentation repository	An area on www.veriffy.com which has been set up for the submission of public documents.

Operational Regulations	This document
PoE	Proof of Existence
Timestamp	Data in electronic form that links other data in electronic form to a specific time, thereby creating evidence that the latter existed at that time
Electronic signature	Electronic data that is attached to or logically linked to other electronic data and is used by the signatory to sign
Electronic seal	Data in electronic form that are connected to or logically linked to other data in electronic form in order to ensure the origin and integrity of the latter
Qualified electronic signature	An advanced electronic signature created using a qualified electronic signature creation device and validated by a qualified electronic signature certificate
Qualified electronic seal	An advanced electronic seal created using a qualified electronic seal creation device and authenticated by a qualified electronic seal certificate
Time-Stamping Authority	(TSA) – a trust service provider that provides time-stamping services
Signatory	A natural person with full capacity who creates an electronic signature
Seal maker	Legal entity that creates the electronic seal
Data Protection Regulations	INFORMATION SYSTEM DATA SECURITY PROVISIONS of UAB iSense Technologies
User Administration Rules	INFORMATION SYSTEM USER ADMINISTRATIVE RULES of UAB iSense Technologies
Information Handling Rules	INFORMATION SYSTEM RULES FOR THE SECURE HANDLING OF ELECTRONIC INFORMATION of UAB iSense Technologies
Business Continuity Plan	INFORMATION SYSTEM BUSINESS CONTINUITY MANAGEMENT PLAN of UAB iSense Technologies
Incident Management Rules	INFORMATION SECURITY INCIDENT MANAGEMENT RULES of UAB iSense Technologies

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 complying with the requirements set out in Annex II of the eIDAS Regulation
Qualified electronic signature certificate	An electronic signature certificate issued by a qualified trust service provider which meets the requirements set out in Annex I to the eIDAS Regulation
ETSI	European Telecommunication Standardisation Institute
OID	Object Identifier
PIN	Personal Identification Number
OCSP	Certificate validation compliant with RFC 6960 recommendations
CRL	Certificate validation compliant with RFC 5280 recommendations

1.4. Document Identification

The Operational Regulations shall be made publicly available in the Documentation Repository. Unique Operational Identifier (OID) – 1.3.6.1.4.1.60536.1.1

1.5. List of Regulatory Documents

- 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);
- The latest version of 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 the General Data Protection Regulation);

- The latest version of the Republic of Lithuania Law on Electronic Identification and Trust Services for Electronic Transactions;
- Resolution of the Republic of Lithuania of 18 February 2016 No. 144 "On the appointment of the body responsible for the supervision of trust services and the body responsible for the establishment, maintenance and publication of the national trust list";
- The latest version of the Republic of Lithuania Law on Legal Protection of Personal Data;
- Order of the Director of the Communications Regulatory Authority of the Republic of Lithuania of 21 June 2018 No. 1V-588 "On the approval of the description of the procedure for granting the status of qualified trust service providers and qualified trust services and their inclusion in the national trusted list, as well as the description of the procedure for submitting reports on the activities of qualified trust service providers";
- Order of the Director of the Communications Regulatory Authority of the Republic of Lithuania of 4 June 2019 No. 1V-594 "On the approval of the description of the procedure for reporting violations of security and/or integrity of trust assurance services";
- ETSI EN 319 403 v2.3.1: Requirements for conformity assessment bodies assessing Trust Service Providers;
- ETSI EN 319 401 v2.3.1: General Policy Requirements for Trust Service Providers;
- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI). Policy requirements for TSP providing signature validation services.

1.6. Organisation Managing the Operational Regulations

UAB iSense Technologies

Legal entity code: 302553999

Address: Mėnulio st. 7, 04326 Vilnius

Website address: www.isense.lt

E-mail address: info@isense.lt

The Operational Regulations shall be approved by the General Manager of UAB iSense Technologies.

1.7. Contact Information

For information on all matters relating to this document and the qualified services provided, please contact UAB iSense Technologies at info@veriffy.com

1.8. Information on Qualified Services

Information on qualified services is available at www.veriffy.com/reliability.

Information on the services provided is regularly reviewed and updated at least once a year.

ISENSE guarantees the availability of the Documentation Repository 99.99% of the time.

ISENSE guarantees the availability of the Services 99.99% of the time.

2. GENERAL PROVISIONS

2.1. Liability

2.1.1. Operational Liability

ISENSE shall be liable for losses incurred by users in accordance with Article 13 of eIDAS and the Republic of Lithuania Law on Electronic Identification and Trust Services for Electronic Transactions.

The liability of qualified service providers is set out in the latest version of eIDAS, in the legislation of the Republic of Lithuania regulating trust services to the extent that it does not conflict with eIDAS, and in the contracts concluded.

2.1.2. Limits of Operational Liability

ISENSE is liable for the quality and availability of the services it provides, but only within the limits of the system it operates.

ISENSE shall not be liable for third party system failures, malfunctions, interruptions (fixed outside of ISENSE's operating limits), which may result in disruptions in the provision, quality and availability of the services.

ISENSE shall not be liable for any failures, malfunctions or interruptions in the Customer's systems that may result in disruptions in the provision, quality and availability of the Services.

2.1.3. Financial Liability

ISENSE shall insure its activities in order to ensure its financial liability obligations in an amount at least equal to the amount set out in Article 10 of the Republic of Lithuania Law on Electronic Identification and Trust Services for Electronic Transactions.

2.2. Legal Provisions and Interpretation

2.2.1. Legal Effect of a Qualified Electronic Signature and Seal

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

2.2.2. Key Legislation

The rights and responsibilities of Qualified Service Participants, the requirements for Qualified Service Providers and their responsibilities shall be governed by the legislation referred to in Clause 1.5 of this document.

2.2.3. Dispute Resolution Procedure

Any disputes between ISENSE and Customers shall be settled by negotiation. If the dispute is not resolved, it shall be settled by court proceedings in accordance with the legislation in force in the Republic of Lithuania.

2.3. Fees for the Provision of Qualified Services

Fees for the provision of qualified services shall be publicly available at www.veriffy.com/reliability.

2.4. Provision of Information

2.4.1. Provision of Information to the Supervisory Authority

- ISENSE shall inform the Supervisory Authority promptly, but at the latest within three business days, of any changes to the provision of its Qualified Trust Services which may affect the quality of the provision of Qualified Services;
- Inform the recipients of the trust services and the Supervisory Body at least three business days in advance of any planned planned works which are likely to disrupt the uninterrupted provision of Qualified Services;
- Submit to the Supervisory Authority an activity report for the preceding calendar year indicating the total number of qualified electronic signatures and qualified electronic seals verified during the preceding calendar year by 1 February of each year.

2.4.2. ISENSE Publicly Available Information

ISENSE's publicly available information includes the following:

- Information on the status of Qualified Service Provision;
- Conditions for the establishment and processing of Qualified Services;
- Price lists for Qualified Services;
- Instructions for users on how to use Qualified Services;
- Summaries of ISENSE performance inspection reports prepared by the authorised bodies;
- Other miscellaneous information of an organisational nature or evidence of sound performance relating to the provision of Qualified Services;
- Various advertisements relating to Qualified Services.

2.4.3. Frequency of Information Updates

The information provided by ISENSE shall be updated at the following times or frequencies:

- Changes shall be made, approved and published in the manner provided for in the Data Protection Regulations;
- Other information to be published and updated (e.g. ISENSE performance review findings, etc.) shall be made available as soon as it is received or prepared within a reasonable time;

- Annual risk assessments, in accordance with the Data Security Regulations, which are carried out once a year to check and inventory the software and hardware used;

3. CONFORMITY ASSESSMENT

The compliance of ISENSE's operations with the proper provision of Qualified Services shall be carried out:

- ISENSE shall be audited by a Conformity Assessment Body every 24 (twenty-four) months in accordance with Article 20(1) of eIDAS;
- the Supervisory Authority may at any time carry out an ISENSE audit or require the compliance body to carry out an ISENSE assessment (at the expense of ISENSE), in order to validate that the services provided are in compliance with the requirements set out in eIDAS in accordance with Article 20(2) of eIDAS;
- Where a supervisory body requires an ISENSE to rectify any violations of the requirements of eIDAS and the ISENSE fails to do so within a period of time set by the supervisory authority, the supervisory authority may, in accordance with Article 20(3) of eIDAS, taking into account, in particular, the magnitude, the duration and the consequences of any such violations, withdraw the status of the qualifications of the ISENSE, or of the ISENSE's service provided by the ISENSE affected by the violation, and shall notify it to the body referred to in Article 20(3) of eIDAS, with a view to updating the trusted listings;

4. CONFIDENTIALITY PROVISIONS

4.1. Personal Data

ISENSE shall processes personal data in accordance with the General Data Protection Regulation and the Republic of Lithuania Law on Legal Protection of Personal Data, which implements 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, insofar as it is not in conflict with the General Data Protection Regulation. Personal Data shall be retained for an appropriate, necessary period of time (including after the termination of ISENSE's

activities), but no longer than is necessary for the purposes of the processing of the data, which shall be notified to the individual, in order to allow the data to be used in legal proceedings and to ensure the continuity of operations.

Personal data shall be destroyed when they are no longer required for the purposes of their processing, except where they are required by law to be transferred to the public archives.

4.2. Sensitive Information

The sensitive information stored and handled in accordance with ISENSE's internal rules is the following:

- the log file;
- records of disruptions to the provision of trust services, if their publication could jeopardise the provision of Qualified Services;
- records of internal and external inspections of ISENSE's activities, if their disclosure could jeopardise the security of ISENSE's services;
- emergency plans;
- information on how to protect hardware and software and how to carry out trust service operations.

4.3. Non-Sensitive Information

- Conditions for the establishment and processing of Qualifying Services;
- Price lists for Qualified Services;
- Instructions for users;
- Summaries of ISENSE performance inspection reports prepared by the authorised bodies.

4.4. Provision of Information to Law Enforcement Authorities

ISENSE sensitive information may be provided to law enforcement officials only in accordance with the requirements of the legislation of the Republic of Lithuania.

5. REQUIREMENTS FOR THE PROVISION OF QUALIFIED SERVICES

5.1. General Requirements for the Provision of Qualified Services

The general requirements for Qualified Suppliers to provide Qualified Services shall be described in ETSI EN 319 401.

Qualified Services, i.e. validation carried out in accordance with the requirements of Articles 32, 33 and 40 of eIDAS. Qualified Services shall 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.

Key requirements for Qualified Services are the following:

- The certificate used to validate the signature was a Qualified Electronic Signature Certificate at the time of signature;
- The qualified certificate was issued by a qualified trust service provider and was valid at the time of signature;
- The signature validation data matches the data provided to the relying party;
- The unique set of credentials representing the signatory in the certificate is properly presented to the relying party;
- If an alias was used at the time of signing, this shall be clearly indicated to the relying party;
- An 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 signature;
- The system used for the validation of the qualified electronic signature shall provide the relying party with the correct result of the validation procedure and shall allow the relying party to identify any security problems;
- Validation of signatures shall be performed in accordance with ETSI TS 119 102-1;
- The signature validation report shall be formatted in accordance with ETSI TS 119 102-2.

5.2. Collection and Storage of Records

5.2.1. Recorded Events

All qualified service booking transactions shall be recorded in a secure transaction log. The log entries shall be kept for at least 10 (ten) years. Recorded service booking transactions shall include the following:

- validation of the type of qualified service;
- time and date;
- unique customer identifier;
- unique identifier for the request;
- logical value of whether the service has been successfully delivered.

The event log of information system components shall be used to analyse the actions of information systems, their users and administrators. The data to be captured shall include the following:

- Information on the switching on, switching off or rebooting of information system workstations, application software and other information system components;
- Actions taken by system administrators to change infrastructure configurations;
- Software update actions.

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

5.2.2. Frequency of Viewing Recordings

The ISENSE system transaction and activity logs shall be reviewed at least once a month. Every major event or occurrence resulting from the malfunctioning of systems must be described. The electronic logs of the event logs of the information system components shall be reviewed in accordance with the terms and procedures laid down in the Data Security Regulations, and shall contain the

electronic information relating to the actions taken by the users and administrators of the information systems.

5.2.3. Recording Retention Period

The logs of operations and activities of the ISENSE system shall be kept in ISENSE for 10 (ten) years, and further storage shall be governed by the latest version of the Republic of Lithuania Law on Documents and Archives.

5.2.4. Recording Protection

The transaction and activity logs of ISENSE systems shall be backed up daily. If the number of entries for a particular log is exceeded, the contents of the log shall be transferred to the archive.

5.3. Data Archiving

The following shall be deposited in the archive:

- logs of system operations and activities;

The archive shall be kept for 10 (ten) years; further storage shall be regulated by the Republic of Lithuania Law on Documents and Archives.

Backups enable the system to be restored after a malfunction. Copies of the following software and data files shall be made for this purpose:

- An installation disc containing the Veriffy system software;
- Veriffy systems transaction and activity logs.

5.4. Security Incident Management

Incidents shall be classified and managed according to ISENSE-approved documents:

- The classification of incidents shall be described in the Incident Management Document;
- Management of critical safety incidents shall be described in the Business Continuity Plan.

ISENSE follows the following procedure for managing security incidents:

- In the event of information system malfunctions/incidents that indicate abnormal or non-compliant performance of information system components, such malfunctions/incidents shall in all cases be recorded in an event log, which shall be archived and protected against damage

and loss, unauthorised or inadvertent modification or destruction, in order to ensure that evidence of criminal offences committed during electronic information security (cyber) incidents is relevant and sufficient for law enforcement authorities to establish the fact of criminal offences and for the perpetrators of criminal offences to be unable to deny it;

- When a fault/incident is registered, it shall be prioritised and identified. During identification, the event record shall be recognised and assigned a category and priority depending on the settings of the specialised event log analysis tools;
- The analysis shall assesses whether an event, or a set of events, at a given point in time, conforms to a set of alert generation rules defined by the specialised event log analysis tools. If, during the analysis, the specialised event log analysis tools determine that a certain event or a set of events at a given point in time satisfies certain defined alert generation rules, then the specialised event log analysis tools shall automatically generate an alert;
- Administrators of information system components must review the alert generated and, if necessary, inform the responsible persons of the alert, its content and circumstances;
- The designated information security officer shall review the alert generated and assess whether it may be related to the security and integrity violations referred to in Article 19(2) of eIDAS. If it is determined that the incident may be related to the security and integrity violations referred to in Article 19(2) of eIDAS, the Security Officer shall convene the Task Force provided for in the Business Continuity Plan without delay, but not later than within 4 (four) hours. The supervisory authority and natural persons or legal entities shall be informed of such incidents in accordance with the procedures described in the Incident Management Document within 24 (twenty-four) hours;
- It shall register the incident in question with a flag indicating that it is related to a violation of security and integrity under Article 19(2) of eIDAS;
- It shall inform the supervisory authority by means of a notification in the prescribed form no later than three business days after the containment or cessation of the recorded violation having a significant impact.

5.5. Cessation of Services

5.5.1. Complete Cessation of Services

ISENSE undertakes to act in accordance with a plan for the cessation of the provision of the Qualified Services agreed upon with the supervisory authority (hereinafter referred to as the Coordinated Plan) prior to the cessation of the provision of the Qualified Services, including, to the extent that it is not inconsistent with the Coordinated Plan, the following actions:

- All relevant persons and organisations, as well as the supervisory authority, must be informed of the cessation of the Qualified Services at least 3 (three) months in advance of the planned date of termination of the Qualified Services;
- In relation to the expected date of cessation of services, but no later than 2 (two) months in advance, provide the following information to the supervisory authority:
    - information about the successor;
    - succession agreement;
    - detailed plan for the cessation of the provision of Qualified Services.
- If the activities are not transferred to a third party following the decision to discontinue the provision of Qualified Services, ISENSE shall ensure that the records of the activities are preserved.

5.5.2. Suspension of Services due to EU Sanctions

The provision of Qualified Services may be ceased if the provision of Qualified Services becomes subject to EU sanctions.

5.6. Involvement of Third Parties in the provision of Qualified Services

ISENSE, when using third-party solutions or services, shall always check and ensure that the technical and organisational measures used by the third party to ensure the quality of the service provision and the security of the information are at least equal to the level of information security required by ISENSE.

Qualified Services shall be delivered using solutions and services offered by Microsoft Azure.

Signature validation report uses qualified time stamps (PoE) supplied by the Kingdom of Belgium - Federal Government (https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/BE/11).

6. PHYSICAL SECURITY CONTROL

Veriffy's information system, operators' workstations and information resources shall be installed and stored in a dedicated area that is physically protected against unauthorised access, destruction or removal of equipment. Access to the core elements of the system shall be monitored. Every entry shall be logged in the Data Centre and the stability of the power supply, temperature and humidity shall be monitored.

The hardware and software for the provision of Qualified Services shall be hosted in a Data Centre where physical access is restricted.

The hardware and software to support the provision of Qualified Services shall be available in the Data Centre, which has an uninterruptible power supply and air-conditioning equipment.

The hardware and software intended to deliver Qualified Services shall be hosted in a Data Centre, which is protected against water flooding.

The hardware and software intended to ensure the provision of Qualified Services shall be available in the Data Centre, which is equipped with automatic fire suppression systems.

Qualified Services shall use cryptographic keys stored in a properly secured Microsoft Azure environment. No copies of cryptographic keys shall be made.

Depending on the importance of the information, media containing archive data and backups shall be stored in fireproof safe.

Paper and electronic media containing information affecting the security of the provision of Qualified Services shall be destroyed after the expiry of the retention period of that information by means of special shredding devices.

Access to the components of the Qualified Service provisioning infrastructure system shall only be available from specific network ports of an IP address.

7. PROCEDURAL SECURITY CONTROL

The positions on which ISENSE depends are the following:

- Information Security Officer. Overall responsibility for enforcing security policy. The responsibilities and functions of the IT Security Officer shall be described in the Data Security Regulations;
- Main Administrator of Veriffy. Responsible for the proper functioning of Qualified Services. Installs and configures the equipment used; sets system and network parameters;
- Assistant Administrator of Veriffy. Stands in for the Main Administrator of Veriffy when needed.

Identification and authentication of ISENSE employees' positions shall be carried out in the following ways:

- By drawing up a list of persons authorised to enter ISENSE premises;
- By establishing a list of people allowed physical access to the Veriffy system and network resources;
- The rules set out in the user administration rules ensure that:
    - each user of the information system is unique and directly linked to a specific person;
    - login data may not be shared with any other person;
    - limited functions (arising from the duties of the person concerned) are provided.

8. PERSONNEL SECURITY CONTROL

Recruitment shall be carried out in accordance with the requirements of the Labour Code of the Republic of Lithuania. Recruitment shall be formalised by an employment contract. The Staff Regulations set out the general qualification requirements for employees.

In addition to the above-mentioned general requirements, it shall be guaranteed that the persons carrying out the duties assigned to ISENSE:

- have signed an agreement on duties and responsibilities;
- have received internal training relevant to the performance of their duties;

- have received training on the protection of personal data and confidential information, are acquainted with the security documents, and have signed an undertaking to keep confidential information confidential, and that they are familiar with the safety documentation;
- have no spent or unspent convictions for intentional offences.

Contracted persons performing tasks (external service providers, software developers, etc.) shall be subject to the same verification procedures that apply to ISENSE employees.

9. REALISATION OF QUALIFIED SERVICE PROVISION

9.1. Technical Realisation

The result of the qualified service is a report on electronic signatures stamped with the advanced electronic seal of UAB iSense Technologies. Format for submitting the Qualified Service Report:

- XML report according to ETSI TS 119 102-2. The report is authenticated by an electronic seal.
- PDF report. The report is authenticated by an electronic seal.

Veriffy software validates electronic signatures prepared in the following formats:

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

The principle sequence for the provision of a Qualified Service according to ETSI TS 119 102-1 is shown in the diagrams:

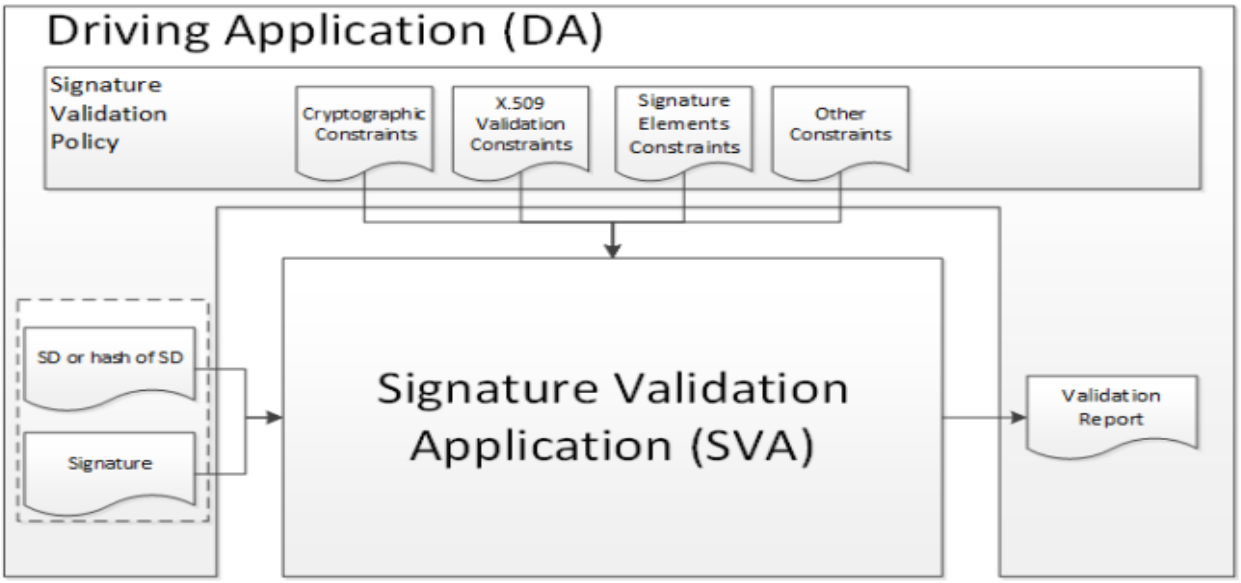

Figure 11: Conceptual Model of Signature Validation

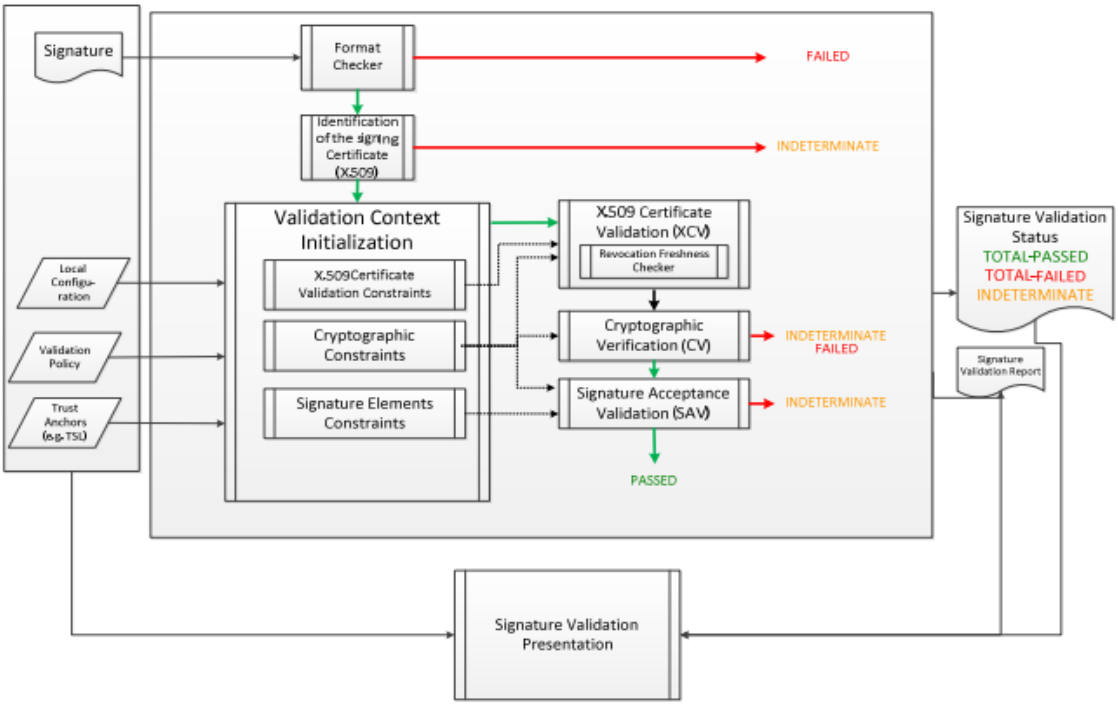

Figure 12: Basic Signature Validation

The authenticity of the signature validation report is confirmed by an electronic seal, additionally marking the signature with a qualified timestamp (PoE).

9.2. Validation Process

According to ETSI EN 319 102-1, three possible signature or seal validation states are given when an electronic signature is validated:

- TOTAL-PASSED: the signature complies with the established validation policy and has passed all validation procedures;
- TOTAL-FAILED: the signature format is incorrect or has not undergone validation procedures;
- INDETERMINATE: signature validation is successful, but there is no information on whether the electronic signature is really valid.

Each validation process provides detailed information on the basis of which the signature status was assigned.

The validation process follows a defined validation policy – electronic signatures are validated for advanced electronic signatures (AdES), signatures validated with qualified certificates (AdES/QC), and fully qualified signatures (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 with CRLs, OCSPs, and timestamps.

The policy on the validation process may be modified by prior agreement of the customer on the required validation elements. In all other cases, the default validation policy is used.

The main aspects of the default QA policy are described in this document and are therefore not further described in any other additional public document.

The procedures described in ETSI TS 119 172-4 shall be followed when validating signature/time stamp certificates. A description of the testing procedure shall be provided in Table 1.

Table 1. Description of the testing procedure

Scenario	Validation status
Signing a document with a qualified signature and a qualified timestamp.	TOTAL_PASSED
Changing the content of a signed document.	TOTAL_FAILED
Signing a document with an unqualified electronic signature or seal.	INDETERMINATE

The result of the validation shall be provided to the customer:

- via the Veriffy API integration interface. When a document is received from a customer for validation, the Veriffy system shall perform the validation without storing the document. After validation, the result shall be transformed into a human/computer readable XML and/or PDF format and the result shall be automatically sealed with the ISENSE seal. This result of the qualified validation can then be used to transform it into other forms. Within the limits of this qualified service, it is unknown what the customer will do with the qualified validation response.
- via the Veriffy portal. Upon receipt of the document from the customer, Veriffy shall carry out a validation. After the validation, the result shall be transformed into PDF format and the result shall be automatically sealed with the ISENSE seal.

9.3. Authenticity Assurance

Once the signatures have been validated, an XML and/or PDF report shall be generated according to ETSI TS 119 102-2. The report shall be signed with this qualified certificate attested by the advanced seal of UAB iSense Technologies.

- Certificatet: C=LT, O= iSense Technologies, UAB, CN=Qualified Validation Service powered by Veriffy
- Issuing authority: C=LT, OU=RCSC, O=SE Centre of Registers – legal entity code 124110246, CN=RCSC IssuingCA
- Certificate serial number: 70944e6fb3a36b2e00000005848c
- Certificate SHA-256 cipher: 72a4a7e72cffef166c4105f6c6d05dca36fd0550

9.4. Method of Provision of Qualified Services

Qualified Services shall be provided in the following ways:

- REST API application integration (service API);
- Web application with User Interface.

10. GENERAL PRINCIPLES FOR THE REALISATION OF QUALIFIED SERVICES

10.1. List of Trusted Suppliers in the European Union

In order to allow each country in the European Union to exchange lists of trusted suppliers, the European Commission shall publish centrally the places of publication of the lists of trusted suppliers for all EU countries. When synchronising lists of trusted suppliers, the authenticity of the information contained in these lists shall be checked. The information contained in the Trusted Supplier Lists shall be used to determine the qualification of certificates for signatures, CRLs, OCSPs and timestamps within the European Union.

10.2. Data and Flows

Qualified Services shall be provided after authentication of the customer. The customer shall be given an authentication key. The customer shall send an electronic document (data) containing signatures/seals, signature certificates, certificate public keys over a secure HTTPS channel. The document shall then be processed according to the selected qualified service – validation, preparation for long-term storage. In order to minimise risk, the document shall only be kept for as long as it is needed to perform a specific qualified service.

Qualified validation shall involve the validation, on receipt of the document and the signatures, that the document has not been altered since it was signed and that the parts that are declared are actually signed. Certificates of the signatory shall be validated. During these validations, the issuing body may be contacted with the identification numbers of the certificate.

The reliability of the certificates shall be checked against a pre-synchronised (once a day) pan-European list of trusted suppliers. Certificate validations shall be carried out on the basis of the issuing body information contained in the signature certificate.

An electronic document and its content can be completely arbitrary and unknown to us in advance. During the validation, the data shall be subjected to automated cryptographic hash operations to validate that the data has not been modified.

Electronic signatures store the signatory's certificate information and its public key. The certificate may contain the person's name, surname, position, nickname, certificate identification

number, personal identification number, etc. This information shall be entered on the certificates by the issuing body. Each certification body shall record different information, depending on national practices, certificate profiles, etc.

When the Qualified Inspection Report is created, it shall be signed with the ISENSE advanced electronic seal. The private key of the press certificate shall be stored in restricted access software. Every use of the electronic seal private key shall be recorded and audited.

All transactions and referrals (from the Customer to the Veriffy information system) shall be audited and stored in a database, linked to the Customer's key.