Advanced Electronic Seal with Qualified Certificate
DOKOBIT
2025-08-12 09:09:29 GMT+3
Purpose: Seal
Dokobit By Signicat

Dokobit
By Signicat

Qualified Signature and Seal Validation Service Practice Statement and Policy v1.15

Document Number: DKB-VSP-06122019 v1.15

Unique object ID (OID): 1.3.6.1.4.1.54720.1.1

Effective from 2025-09-12

© 2025 — Dokobit, UAB — e-signing as an everyday service.

https://www.dokobit.com

Table of Contents

1 Change history 5
2 Introduction 7
2.1 Overview 7
2.1.1 TSP identification 8
2.1.2 Supported validation service policy 8
2.2 Validation service components 8
2.2.1 SVS actors 8
2.2.2 Service architecture 9
2.3 Definitions and abbreviations 10
2.3.1 Definitions 10
2.3.2 Abbreviations 11
2.4 Policies and Practices 12
2.4.1 Organisation administering the TSP documentation 12
2.4.2 Contact Person 13
2.4.3 TSP documentation applicability 13
Validation Service Practice Statement and Service Policy 13
Terms and conditions 13
Risk assessment and information security policy 13
2.4.4 Limitation on the use of Dokobit Qualified Validation Service 14
3 Trust Service management and operation 15
3.1 Internal organisation 15
3.1.1 Organisation reliability 15
3.1.2 Segregation of duties 15
3.2 Human resources 16
3.3 Asset management 16
3.3.1 General requirements 16
3.3.2 Media handling 17
3.4 Access control 17
3.5 Cryptographic controls 17
3.6 Physical and environmental security 18
3.7 Operation security 18
3.8 Network security 19

3.9 Vulnerabilities and incident management ... 19
3.9.1 Monitoring and logging ... 19
3.9.2 Incident response ... 19
3.9.3 Reporting ... 19
3.9.4 Event assessment and classification ... 20
3.9.5 Post-incident reviews ... 20
3.10 Collection of evidence ... 20
3.11 Business continuity management ... 21
3.11.1 General ... 21
3.11.2 Back up ... 21
3.11.3 Crisis management ... 21
3.12 TSP Termination and termination plans ... 22
3.13 Compliance ... 22
3.14 Supply chain ... 22
4 Validation service design ... 23
4.1 Signature validation process requirements ... 23
4.1.1 Signature validation model ... 24
4.1.2 Status indication of the signature validation process and the signature validation report ... 25
4.1.3 Validation process ... 33
4.1.4 Validation constraints for electronically signed documents ... 34
General Constraints ... 34
X.509 Validation Constraints ... 35
Cryptographic Constraints ... 37
Signature and Seal Elements Constraints ... 37
4.2 Signature validation protocol requirements ... 38
4.3 Interfaces ... 39
4.3.1 Communication channel ... 39
4.3.2 SVSP - Other Trust Service Providers ... 39
4.4 Signature validation report requirements ... 39
5 Annex A ... 41
6 Annex B ... 47

Document Number: DKB-VSP-06122019 v1.15

Unique object ID (OID): 1.3.6.1.4.1.54720.1.1

Effective from 12.09.2025

1 Change history

Date	Version	Description of change
03/08/2018	1.0	Initial version for Dokobit Signature Validation Service
10/10/2019	1.2	Revamped document to meet the requirements set in ETSI TS 119 441
03/12/2019	1.5	• Updates to become compliant to the recommended document structure (Annex A of ETSI TS 119 441 V1.1.1 (2018-08)) • Associations to ISO27001 SoA document
06/12/2019	1.6	Added signature validation service components and service architecture diagram, necessary changes for provision of Qualified Trust Service
17/04/2020	1.7	Minor updates • Clarified 2.1.2 section - OID is for the Policy document • Added Qualified Trust Service Provider OID in 2.1.1 • 4.1.3 and 4.3.1 changed to reflect that the user authenticates to the service using electronic identification means. • Added Notification to Supervisory Body clause in 2.4.3 • Defined the use of a pseudonym in Signature Validation Reports in 4.1.2 • Added SVS termination notice period in 3.12 • Clarified a list of applicable legal acts of the Republic of Lithuania in 2.1
26/11/2020	1.8	• Added extended descriptions in Trust Service management and operation sections to be more readable for third-parties • Added new Driving Application and extended Driving Application descriptions in Signature Validation model in 4.1.1 • Added the use of Dokobit Validation Service in clause 4.1.3 • Added the use of Dokobit Validation Service in clause 4.2 • Added the use of QWAC certificate in clause 4.3.1
01/05/2021	1.9	• Added Limitation on the use of Dokobit Qualified Validation Service under 2.4 Policies and Practices • Added Validation Policy constraints in Annex A and Annex B
08/07/2021	1.10	• Amended document name with “Seal” - Qualified Signature and Seal Validation Service Practice Statement and Policy
07/11/2022	1.11	• Change of company’s registration address.
05/06/2023	1.12	• Added UA TSL.

Date	Version	Description of change
08/05/2024	1.13	• Updated references to the legal acts. • Updated responsibilities for documentation approval. • Included new constraint (level WARN) regarding detected elements that might change the visual appearance of the signed document. • Removed fixed TL freshness constraint • Minor corrections for better readability.
09/01/2025	1.14	• Updates due to updated Dokobit ISMS and transition to new versions of standards, ISO/IEC 27001:2022 and ISO/IEC 27002:2022. • Updates due to new versions of ETSI EN 319 401 and ETSI TS 119 441 • Updates due to eIDAS v2 and the NIS 2 Directive with resulting Lithuanian law
30/06/2025	1.15	• Updates due to Dokobit, UAB changing from a separate ISMS to a common ISMS of the Signicat Group. • Minor corrections for better readability. • Minor corrections related to branding changes.

2 Introduction

2.1 Overview

This document describes the practices applied by Dokobit, UAB (hereafter Dokobit) in providing the **Qualified Signature and Seal Validation Services** (hereafter Qualified Validation Service) in conformity with:

- *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 (eIDAS v1), as amended by *Regulation (EU) 2024/1183* of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework into the consolidated text *Amended eIDAS regulation* (eIDAS v2)
- *Directive (EU) 2022/2555* of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
    - *Commission implementing Regulation C(2024) 7151* laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers, and its *Annex*
- *Directive (EU) 2019/882* of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services
- Legal acts of the Republic of Lithuania:
    - Law of The Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions
    - On the approval of the specification of the procedure for granting the 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 by Order No. 1V-588 of the Director of the Communications Regulatory Authority on April 21, 2018
    - The Description of the Procedure for Reporting Breaches of the Security and/or Integrity of Trust Services and Approved ID Tools approved by Order No. TN-708 of the Board of the Communications Regulatory Authority on 21 December 2023
    - The *Law No. XII-1428 of the Republic of Lithuania on Cyber Security*, as amended by *Law No. XIV-2902 on Amendment of the Law No. XII-1428 of the Republic of Lithuania on Cybersecurity* (NIS 2 in Lithuanian law)
- European standard *ETSI EN 319 401* Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers, V3.1.1, June 2024
- ETSI Technical Specification *ETSI TS 119 441* Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services, V1.2.1, October 2023
    - The structure of this document is compliant to Annex A of ETSI TS 119 441
- ETSI Technical Specification *ETSI TS 119 442* Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services, V1.1.1, February 2019

- European standard *ETSI EN 319 102-1* Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, V1.4.1, June 2024
- ETSI Technical Specification *ETSI TS 119 102-2* Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report, V1.4.1, June 2023
- ETSI Technical Specification *ETSI TS 119 172-1* Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents, V1.1.1, July 2015
- ETSI Technical Specification *ETSI TS 119 172-4* Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists, V1.1.1, May 2021
- ETSI Technical Specification *ETSI TS 119 312* Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites, V1.5.1, December 2024

2.1.1 TSP identification

Dokobit, UAB

Company code 301549834

Paupio g. 50-136, LT-11341 Vilnius

Email *info@dokobit.com*

www.dokobit.com

The registered formal object identifier (OID) - 1.3.6.1.4.1.54720

2.1.2 Supported validation service policy

The Qualified Signature and Seal Validation Service Policy is identified with a registered formal object identifier (OID) 1.3.6.1.4.1.54720.1.1

This policy is based on the qualified validation policy defined in ETSI TS 119 441 with the OID 0.19441.1.2

The variances of the Dokobit Qualified Signature and Seal Validation Service Policy towards the policy defined by ETSI TS 119 441 are that the Dokobit document is also a practice statement, plus the sections on specification of limitations/liabilities of use, validation report requirements, validation constraints, and formats supported.

2.2 Validation service components

2.2.1 SVS actors

Signature Validation Client (SVC)

- A software component that provides a user interface for the Driving Application used by Dokobit Service Subscribers.

Driving Application (DA)

- An application which provides signature validation functionality to the Signature Validation Client.

Signature Validation Service Protocol (SVP)

- Secure communication channel for exchanging information with the Signature Validation Service Server (SVSServ).

Signature Validation Service Server (SVSServ)

- The component that implements the signature validation protocol on the SVSP's side.

Signature Validation Application (SVA)

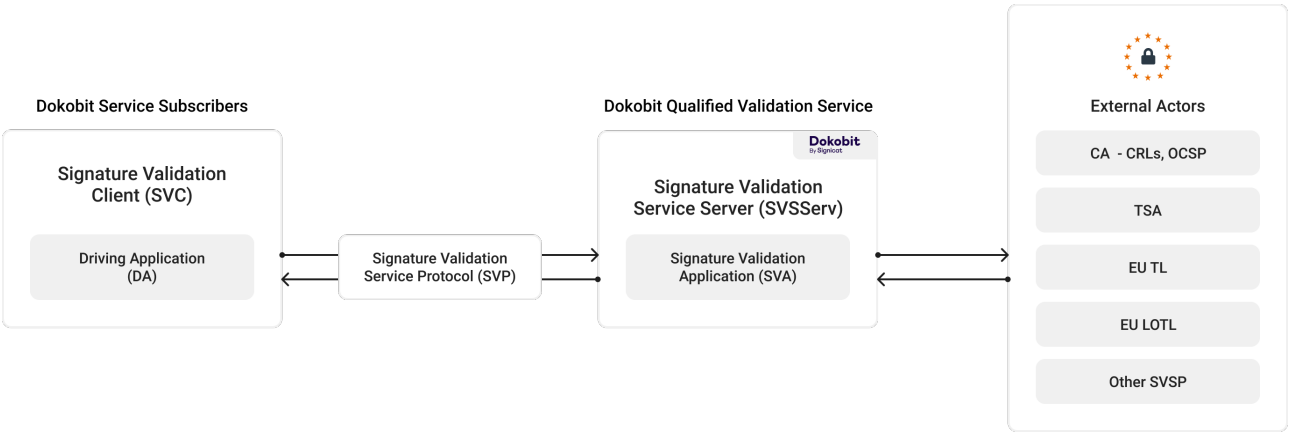
- A software component responsible for signature validation, which implements the validation algorithm and creates a signature validation report.

External Actors

- Other trust sources - Certification Authorities, Time-stamping authorities, European Trusted List providers, and the European Commission providing the list of Trusted Lists, which are called to fulfil their purpose.

2.2.2 Service architecture

The diagram below displays the simplified Dokobit Qualified Validation Service architecture and involved actors.



2.3 Definitions and abbreviations

2.3.1 Definitions

Name	Abbreviation	Definition
eIDAS Regulation	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, as amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
General Data Protection Regulation	GDPR	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 (General Data Protection Regulation).
Network and Information Systems Directive	NIS 2	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
Information Security Management System	ISMS	Information Security Management System of Signicat Group, which is certified according to ISO/IEC 27001:2022. Dokobit, UAB is included within the scope of certification as detailed in the certificate annex listing covered subsidiaries.
Trust Service Provider	TSP	An entity which provides a Trust Service.
Qualified Trust Service Provider	QTSP	An entity that provides one or more Qualified Trust Services and is granted qualified status by the Supervisory Body.
Supervisory Body		The authority that is designated by a member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS in the territory of that member state.
Dokobit Validation Service Practice Statement		A statement of the policy and practices Dokobit employs in providing the Qualified Validation Services.

Name	Abbreviation	Definition
Signature Validation Service	SVS	Trust Service for Signature and/or Seal Validation.
Relying Party	RP	A natural or legal person that relies on the Trust Service.
Signicat Group		Signicat AS and its subsidiaries, including Dokobit, UAB.
Subscriber		A legal or natural person bound by an agreement with Dokobit to any Subscriber obligations.
Certification Authority	CA	Trust Service Provider that issues certificates for electronic signatures and/or seals.
Qualified Certification Authority	QCA	Qualified Trust Service Provider that issues qualified certificates for electronic signatures and/or seals.

2.3.2 Abbreviations

DA	Driving Application
PoE	Proof of Existence
QES	Qualified Electronic Signature or Qualified Electronic Seal
AdES	Advanced Electronic Signature
AdES/QC	Advanced Electronic Signature created with a Qualified Certificate
(Q)SCD	(Qualified) Signature Creation Device
QSVSP	Qualified Signature Validation Service Provider
SD	Signer's Document
SDO	Signed Data Object
SDR	Signed Document Representation

SVA	Signature Validation Application
SVP	Signature Validation Protocol
SVR	Signature Validation Report
SVSP	Signature Validation Service Provider
SVSServ	Signature Validation Service Server
TSA	Time stamping Authority
VPR	Signature Validation Process
OID	Object Identifier
PKI	Public Key Infrastructure
OCSP	Online Certificate Status Protocol
HSM	Hardware Security Module
ISM	Information Security Manager (CISO of the Signicat Group)
qVAL Director	Director of the Qualified Signature and Seal Validation Services
ISMS	Information Security Management System

2.4 Policies and Practices

2.4.1 Organisation administering the TSP documentation

This document is administered by Dokobit.

Dokobit, UAB

Company code 301549834

Paupio g. 50-136, LT-11341 Vilnius

Email *info@dokobit.com*

www.dokobit.com

2.4.2 Contact Person

The contact person for the management of this document shall be the Director of the Qualified Signature and Seal Validation Service of Dokobit.

Further information can be requested via email *compliance@dokobit.com*.

2.4.3 TSP documentation applicability

Validation Service Practice Statement and Service Policy

Dokobit is responsible for the management of the Dokobit Validation Service Practice Statement, which covers the Service Policy. This document shall be approved by the management and made public on the Dokobit Compliance website (*https://www.dokobit.com/compliance*).

Dokobit shall notify the Supervisory body about any changes in the provision of qualified trust services without undue delay, but no later than 3 working days. Dokobit shall notify the Supervisory body about the planned termination of the qualified trust service no less than 3 months before the termination of the qualified trust service.

Notification to the Supervisory Body shall be sent without undue delay and not later than 3 working days after any changes in the Dokobit Validation Service Practice Statement.

Subscribers and Relying parties shall only take into account the effective version of the Dokobit Practice Statement as of the time of using the services provided by Dokobit. A new version of the Dokobit Practice Statement, along with enforcement dates, is published at least 30 days before taking effect.

Terms and conditions

Dokobit makes the Terms of Service as well as the Data Processing Agreement available on the Dokobit Compliance website (*https://www.dokobit.com/compliance*).

Risk assessment and information security policy

Dokobit operates under the Information Security Management System (ISMS) of Signicat Group. Signicat AS, the parent company of Dokobit, UAB, has achieved certification of ISMS according to ISO/IEC 27001:2022 standard with the certification scope of “Providing digital identity and electronic signature solutions, including Qualified Trust Services (qualified timestamps, qualified signature and seal validation, and qualified certificate issuance for qualified electronic signatures) using ISO/IEC 27018:2019 and in accordance with

Statement of Applicability latest version". Dokobit, UAB is included within the scope of certification as a subsidiary.

The ISMS and the ISO/IEC 27001:2022 certification cover risk assessment and risk treatment methodology, and Information Security, Organisation of Information Security and Compliance policies. The Policies and the risk assessment methodology are applied for the Qualified Validation Service. The risk assessment includes threat intelligence.

All necessary controls required by eIDAS, GDPR and other relevant legal acts and corresponding standards (i.e. ETSI EN 319 401) are implemented and maintained within the ISMS. Furthermore, in the context of NIS 2, Dokobit, UAB, is classified as an essential entity and is required to operate under the compliance measures outlined by the National Cyber Security Centre of the Republic of Lithuania.

Signicat Group's Information Security Board (ISB) approves policies and practices related to information security, whereas qVAL Director is responsible for approving Qualified Validation Service-related policies and practices.

2.4.4 Limitation on the use of Dokobit Qualified Validation Service

Dokobit Qualified Validation Service provides Validation Reports with three different limitations:

- Tier 1 (Basic Liability). This tier is for documents that don't exceed the value of EUR 100 as Dokobit will be liable up to EUR 100 per Validation Report.
- Tier 2 (Advanced Liability). This tier is for documents that don't exceed the value of EUR 10 000 as Dokobit will be liable up to EUR 10 000 per Validation Report.
- Tier 3 (Premium Liability). This tier is for the documents that don't exceed the value of EUR 100 000 as Dokobit will be liable up to EUR 100 000 per Validation Report.

Limitations shall be stated in each Validation Report generated by Dokobit Qualified Validation Service.

3 Trust Service management and operation

Dokobit operates under the Information Security Management System (ISMS) of Signicat Group, which has achieved *ISO/IEC 27001:2022 certification* by an accredited international certification body. Dokobit is included as a subsidiary in the ISO/IEC 27001:2022 certificate of Signicat AS (the parent company of the Group). Qualified Validation Service is within the scope of this certification. The ISMS covers all applicable controls specified in ISO/IEC 27001:2022 Annex A. These controls are from ISO/IEC 27002:2022, which is the basis for the controls of the ETSI EN 319 401 standard, hence, the ISMS covers the ETSI EN 319 401 requirements in general. Additionally, controls from the ISO/IEC 27018 ensuring the highest protection of personal data in cloud environments have been implemented.

The paragraphs below summarise the management and operations of the trust service.

3.1 Internal organisation

Dokobit complies with all legal obligations applicable to the provisioning of its Trust Services. It conducts its operations in line with the adopted policies and practices, which are according to requirements from applicable standards. Dokobit ensures that all requirements defined in the ISMS Statement of Applicability and this Practice Statement are implemented and remain applicable to the Trust Services provided.

The provision of Trust Services is subject to an external audit performed at least every 24 months by a Conformity Assessment Body (CAB).

3.1.1 Organisation reliability

Dokobit has the necessary financial stability and resources for operation in accordance with this document. Dokobit maintains insurance of its civil liability in accordance with the applicable legislation, to cover obligations arising from its operations and in line with Article 13 of eIDAS regulation. Dokobit may provide more information about specific organisation reliability measures upon a special legitimate request from the concerned party.

3.1.2 Segregation of duties

The ISMS ensures that the necessary segregation of duties is verified and maintained. Specifically for the Qualified Validation Service, the roles of Information Security Manager (ISM), qVAL Director, and Internal Auditor are separated. The four eyes principle is ensured in vital areas:

- Secure development and code reviews
- Software deployment

3.2 Human resources

The ISMS ensures that all required human resource controls are implemented. The controls are documented in the ISMS Statement of Applicability and cover the following topics:

- Background screening
- Terms and conditions of employment
- Non-disclosure after termination or change of employment
- Training and qualifications of staff
- Disciplinary sanctions
- Definitions and job descriptions for trusted roles
- Procedures and responsibility for appointment to trusted roles (responsibility of management and qVAL Director)
- Remote working

The employees and contractors receive adequate training and have all the necessary experience for carrying out the duties specified in employment or contractor agreements as defined in the Human Resources Security policy for Signicat Group.

3.3 Asset management

3.3.1 General requirements

Dokobit maintains up-to-date lists of assets, incl. information assets, with assigned ownership to all assets. Risk Management is based on the identification of assets. Risk Assessment is aligned with the identification of assets, and threats are identified as related to assets using elaborate mapping. Assets are classified according to requirements for protecting confidentiality, integrity, and availability.

Asset management is part of Signicat Group's ISMS, including Acceptable Use Policy, Information Classification Policy and Risk Management Methodology. Personnel and other parties are required to return assets upon change or termination of employment.

The Qualified Validation Service, as an asset, as well as other core assets for the service, are owned by the qVAL Director.

3.3.2 Media handling

Media containing sensitive information is handled securely and in accordance with Asset Management, Communications Security and Operations Security Policy parts of the ISMS. Media handling for the operational Qualified Validation Service is carried out by the cloud hosting operator.

3.4 Access control

Access Control Policy, which is a part of Signicat Group's ISMS, ensures that system access shall be limited to authorised individuals and that all necessary controls for secure access are implemented.

The basic principle applied in access controls is that access to all systems, networks, services, and information is denied by default, unless explicitly permitted on a need-to-know basis to individual users or groups of users. Any access granted is further restricted according to the principle of least privilege. The Access Control Policy provides a comprehensive framework for (electronic) access provision, requirements for corporate account security settings, privilege management, and regular review of access rights. According to the policy, associate traceable access control records must be ensured and kept. Remote access is supported in an encrypted manner only (as per the Mobile Devices & Teleworking Policy) and is subject to the Acceptable Use Policy.

The Access Control Policy provides a framework for registration of a user in the corporate directory, internal network, and information systems. Also, recommended technical (security) parameters supplement the user registration process. The Access Control Policy also defines a user de-registration process, including requirements for account removal. Authorisation for access must be granted by the system (asset) owner and, depending on the information classification of the processes and information that are to be protected, additionally be authorised by management.

Acceptable Use Policy provides comprehensive requirements for users to manage and use secret authentication information. It enforces best industry practices, like enforced 2FA and encrypted password management tools. Detailed requirements for corporate account security settings are listed in the Access Control Policy, which reflects industry best practices.

3.5 Cryptographic controls

Cryptographic controls are defined following the cryptography policy, which is part of the ISMS. Communication towards the Qualified Validation Service is secured by the TLS protocol using approved

cryptography. Sealing of validation reports is done by approved cryptography with the private key stored in an HSM provided by the cloud hosting operator.

3.6 Physical and environmental security

The Operations Security Policy covers physical access to information assets and local equipment. The physical and environmental security of the equipment used to provide the Qualified Validation Service is handled by the cloud hosting provider, regulated by the contractual clauses and subject to the Supplier Relationship Policy.

Relevant in-house equipment is located in secure areas only. The Scope document for the ISMS describes a list of secure areas and associated protection controls and procedures.

The physical security perimeter for Dokobit premises is defined in the Scope document for the ISMS. Based on the risk assessment, controls of physical security are implemented to ensure the required level of protection. Physical security controls are subject to comprehensive risk management and assessment activities. In general, there are different levels of physical entry controls defined in the Access Control Policy and Physical and Environmental Security Policy that depend on the facility's vitality. For example, access to secure areas is “denied by default” (e.g. locked) except permitted. Due to the nature of Dokobit activities and the use of public cloud IaaS providers, the company is not reliant on one or a few fixed physical locations.

Public access areas, including the delivery and loading zone (entrance to the office building), are controlled by the office building's security guard at daytime and locked at night.

3.7 Operation security

The Signicat Group’s ISMS covers this section via the Operations Security Policy, Communications Security Policy, System Acquisition, Development and Maintenance Policy, Supplier Relationship Policy, Incident Management Policy, Access Control Policy, Mobile Devices & Teleworking Policy, and Privacy Policy. The documentation covers, among others:

- Change control
- Malware protection
- Authentication, authorisation, and access control
- Patching
- Configuration management
- Monitoring and alarms
- Configuration and other reviews

3.8 Network security

The Signicat Group's ISMS covers this section via the Operations Security Policy and Communications Security Policy. Segregation in networks is emphasised. As a result,-production, staging/pre-production, development/test, and office support environments are segregated. Network connections and ports are by default closed and opened only on explicit demand. Vulnerability scans and penetration testing are carried out routinely.

3.9 Vulnerabilities and incident management

3.9.1 Monitoring and logging

The Signicat Group's ISMS covers this section via the Operations Security policy, which includes comprehensive monitoring, alarm, and logging procedures. Security logs are regularly reviewed to support the detection and investigation of suspicious events in production and corporate systems. All logs are sent to remote log aggregator systems.

3.9.2 Incident response

This section is covered by Signicat Group's ISMS via the Incident Management Policy and by the Dokobit Incident Management Procedure. Incident Management Procedure represents a comprehensive workflow for managing information security incidents. The procedure is aligned with the GDPR, NIS 2 and eIDAS requirements set for Qualified Trust Service Providers, relevant to the context, and represents all necessary responsibilities across Dokobit for reporting and handling an incident. Lessons learned from previous incidents are integrated into Dokobit operations. The Incident Management Procedure includes sections on Incident Containment and Eradication and Incident Recovery.

3.9.3 Reporting

As per Signicat Group's Incident Management Policy and Dokobit Incident Management Procedure, information security events might be detected internally by Dokobit controls or reported by internal or external parties.

The initial analysis phase of the Incident Management Procedure defines assessment criteria for a security event. If an event is confirmed as a security incident, it triggers further response actions (documented in the procedure) based on best international practices (primarily ENISA, GDPR, NIS 2 and eIDAS guidelines).

ISM and qVAL Director are responsible for contacts with authorities relevant to information security, such as CERT institutions, the Personal Data Protection Inspectorate, and the Supervisory Body under the eIDAS Regulation. The Incident Management Procedure provides a special communication protocol in the form of predefined templates to ensure contact with authorities in a timely, precise, and compliant with applicable laws manner during the event of an incident. Applicable laws are defined in the List of Legal, Regulatory, Contractual and Other Requirements.

ISM and qVAL Director are responsible for contacts with special interest groups relevant to their role in information security. Furthermore, ISM owns the Responsible Vulnerability Disclosure policies, which enable community-based ("white and grey hats") vulnerability identification in Dokobit assets.

3.9.4 Event assessment and classification

The initial analysis phase of the Incident Management Procedure defines assessment criteria for a security event. An event is reclassified if information during the event handling indicates that the event is more or less severe than the conclusion of the initial analysis.

3.9.5 Post-incident reviews

The Incident Management Procedure defines post-incident activities, where lessons-learned analysis is performed, which might result in risk reassessment, controls review, ISMS documentation update, or some specific improvement actions.

3.10 Collection of evidence

Dokobit applies the requirements specified in clause 7.10 of ETSI EN 319 401 with respect to the collection of evidence. These records will only be disclosed to law enforcement authorities under court order and to persons with a legitimate request. Such information is managed in line with the Privacy and Compliance Policies, which are a part of Signicat Group's ISMS.

Specifically for incidents, the Incident Management Procedure parts on Incident Containment and Eradication and Incident Recovery specify evidence collection in the event of an incident or after it.

3.11 Business continuity management

3.11.1 General

Dokobit has implemented a Disaster Recovery / Business Continuity Plan and is covered under the group-wide crisis management arrangements, which are a part of the Signicat Group's ISMS. The purpose is to define precisely how Dokobit will recover its services within set deadlines in the case of a disaster or other catastrophic event identified during the risk assessment. The objective of this plan is to complete the recovery of services within the set recovery time objective (RTO) and Recovery Point Objective (RPO). The plan precisely addresses roles, responsibilities, and, when activated, triggers the restoration of services in an alternative pre-selected location in an automated manner specific to every service plan.

The Disaster Recovery / Business Continuity Plan addresses all relevant aspects of information security continuity and incorporates them into associated procedures. The dedicated section of the plan on Information Security Continuity Aspects clarifies those aspects.

The Disaster Recovery / Business Continuity Plan is based on the risk scenarios for certain assets identified during the risk assessment. Based on the security requirements, the DR/BC plan has set the RTO and RPO of information required to support activities during disruption.

Due to the nature of Dokobit's activities and its native orientation to cloud services, Dokobit's information security is resilient to disruptive events.

3.11.2 Back up

The Operations Security Policy defines requirements and routine activities for information backups. Backup copies are ensured for all Dokobit online products and the services provided for clients. The backup process is automated, fully aligned and tested to comply with declared RPOs and RTOs for services' restoration in the event of interruption or disaster. In addition, Dokobit verifies and tests the integrity of backups as part of its routine operations.

3.11.3 Crisis management

This is covered by the Signicat Group's crisis management plan. Furthermore, the threat intelligence processes of Dokobit target early discovery of threats that can potentially cause a crisis.

3.12 TSP Termination and termination plans

Dokobit has an up-to-date termination plan in accordance with clause 7.12 of ETSI EN 319 401. The termination plan includes procedures to inform all relevant parties of the termination and provisions to ensure the continued availability of needed information.

Dokobit has additional third-party warranties to cover the costs to fulfil these minimum requirements in case the TSP goes bankrupt, or for other reasons is unable to cover the costs by itself.

Dokobit reserves the right to terminate the provisioning of the Validation Service by informing Customers and the Supervisory body with a minimum notice of 3 months.

3.13 Compliance

This section is covered by Signicat Group's ISMS via the Compliance Policy. The procedure defines the process of identification of interested parties, as well as legal, regulatory, contractual and other requirements and responsibilities for their fulfilment. Legal and standards documents that are relevant for compliance of the Qualified Validation Service are listed at the beginning of this Practice Statement. Access for people with disabilities is a compliance requirement for all Dokobit services.

3.14 Supply chain

Signicat Group's ISMS includes a Supplier Relationship Policy, applied for the screening and management of all suppliers. The checks of supply chain integrity ensure that the underlying code and binaries in 3rd party components used in Dokobit services are verified and that they pass attestation tests. All suppliers undergo a security assessment, which includes sub-suppliers involved.

All contracts with suppliers have a contract owner, who is responsible for regular (annual in most cases) checks on the status of suppliers. In case of an indication of contract break or increased risk, the contract owner may request an audit of the supplier.

In compliance with GDPR, Dokobit signs (accepts after evaluation) the Data Processing Agreements with sub-processors.

4 Validation service design

The service may only be used by Dokobit contractual customers. The Service can only be accessed using defined interfaces and applications published by the validation service provider.

The Subscriber of the Service is obligated to protect the Service interface from unauthorised use and provide appropriate security when using the Services. This applies to any interface used to access the Service.

This Interface means, in particular, the web application for using the Service or any application or integration interface supplied exclusively by Dokobit or an integrator specified by the Service provider.

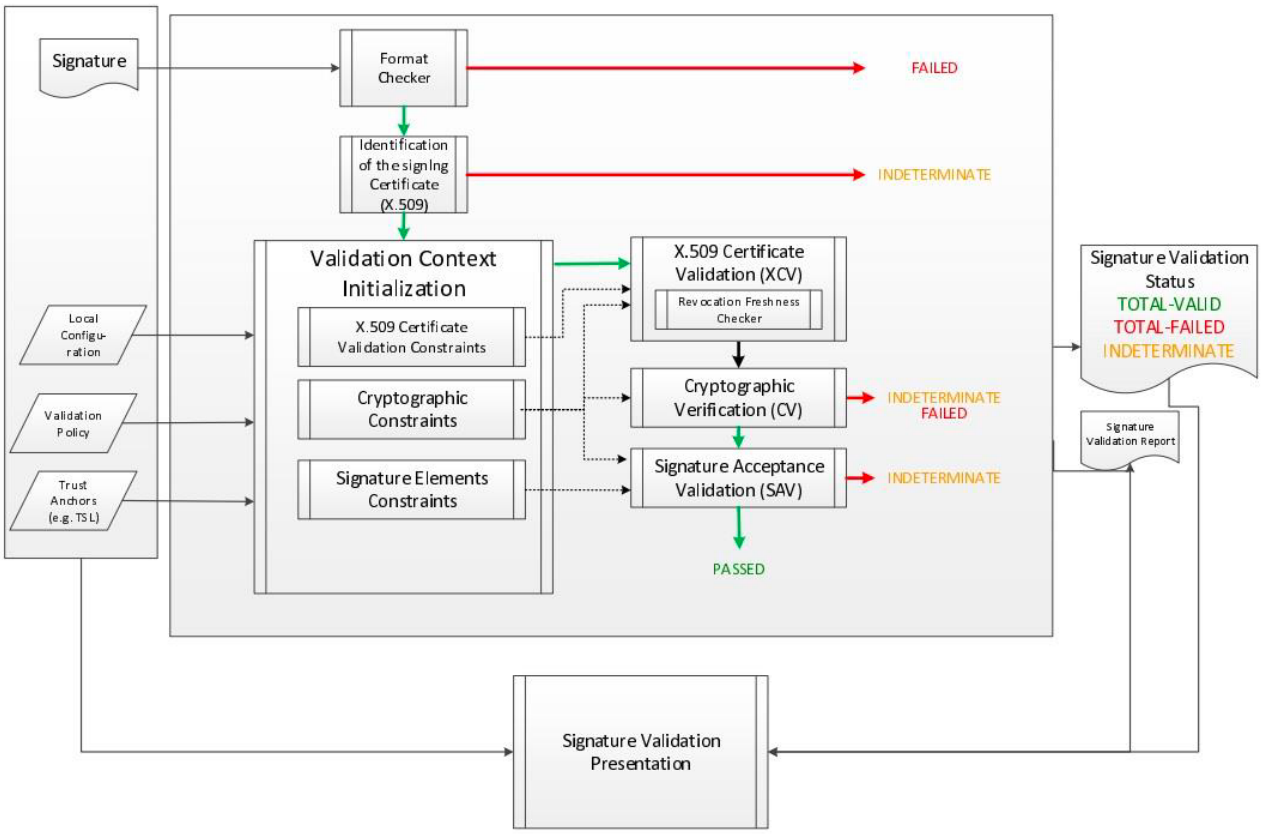
4.1 Signature validation process requirements

Dokobit validation service procedures for establishing whether an electronic signature or electronic seal is technically valid rely on the process described in ETSI EN 319 102-1.

The following sections explain the way the Dokobit validation service performs individual components of validation procedures, indicating the processes occurring and constraints. When no specific requirement is set in the present document, requirements and rules from ETSI EN 319 102-1 clause 5 shall apply in their entirety.

When specific requirements and rules are set in the present specification, they shall prevail over the corresponding requirements from ETSI EN 319 102-1. In case of discrepancies between the present specifications and specifications from ETSI EN 319 102-1, the present specifications shall prevail.

4.1.1 Signature validation model



According to the conceptual model of Signature Validation defined in the referenced specification, Dokobit Validation Service acts as an SVA. The SVA is called by the Driving Application (DA), to which it has to return the results of the validation process, in the form of a validation report.

The Driving Application (DA) for the Dokobit Validation service could be:

- Dokobit Portal - available at *https://app.dokobit.com*
- Dokobit Validation Service - available at *https://validation.dokobit.com* and via integrations in other information systems.
- Dokobit Gateway - available at *https://gateway.dokobit.com*
- Dokobit Validation Service API

Dokobit Validation service accepts only one file for validation, which should contain signatures and signed content files in it.

4.1.2 Status indication of the signature validation process and the signature validation report

Dokobit validation service provides a comprehensive report of the validation, allowing the DA to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the service.

Dokobit Portal, Dokobit Validation Service and Dokobit Gateway present the report in a meaningful way to the user – a human-readable HTML page with the ability to download a sealed signature validation report.

The signature validation process output contains:

- list of signatures;
- a status indicating the results of the signature validation process;
- errors describing why the signature is invalid (TOTAL-FAILED) or warnings describing why SVS was unable to determine the signature status (INDETERMINATE);
- an indication of the policy in which the signature has been validated;
- the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing/sealing;

According to the algorithm specified in ETSI EN 319 102-1, the signature validation status can be:

Table 1 Validation report structure and semantics

Status indication	Semantics	Associated Validation report data
TOTAL-PASSED	The signature validation process results in TOTAL-PASSED based on the following considerations: • the cryptographic checks of the signature succeeded (including checks of hashes of individual data objects that have been signed indirectly); • any constraints applicable to the signer's identity certification have been positively validated (i.e. the signing certificate consequently has been found trustworthy); and • the signature has been positively validated against the validation constraints and hence is considered conformant to these constraints.	The validation process outputs the signing certificate, used in the validation process, together with a specific signed attribute, if present, and considered validation evidence.

Status indication	Semantics	Associated Validation report data
TOTAL-FAILED	The signature validation process results in TOTAL-FAILED because the cryptographic checks of the signature failed (including checks of hashes of individual data objects that have been signed indirectly), or it has been proven that the generation of the signature took place after the revocation of the signing certificate.	The validation process outputs additional information to explain the TOTAL-FAILED indication for each of the validation constraints that have been taken into account and for which a negative result occurred.
INDETERMINATE	The available information is insufficient to ascertain whether the signature is TOTAL-PASSED or TOTAL-FAILED	The validation process outputs additional information to explain the INDETERMINATE indication and to help the verifier identify what data is missing to complete the validation process.

In addition to the main status, the signature validation report also includes a secondary indication with the following semantics:

Table 2. Validation report structure and semantics

Main indication	Sub-indication	Associated Validation report data	Semantics
TOTAL-FAILED	FORMAT_FAILURE	The validation process shall provide any information available explaining why the parsing of the signature failed.	The signature is not conformant to one of the base standards to the extent that the cryptographic verification building block is unable to process it.

Main indication	Sub-indication	Associated Validation report data	Semantics
	HASH_FAILURE	The validation process shall provide: An identifier (s) (e.g. a URI or OID) uniquely identifying the element within the signed data object (such as the signature attributes, or the SD) that caused the failure.	The signature validation process results in TOTAL-FAILED because at least one hash of a signed data object(s) that has been included in the signing process does not match the corresponding hash value in the signature.
	SIG_CRYPTO_FAILURE	The validation process shall output: The signing certificate used in the validation process.	The signature validation process results in TOTAL-FAILED because the signature value in the signature could not be verified using the signer's public key in the signing certificate.
	REVOKED	The validation process shall provide the following: • The certificate chain used in the validation process. • The time and, if available, the reason of revocation of the signing certificate.	The signature validation process results in TOTAL-FAILED because: • the signing certificate has been revoked; and • there is proof that the signature has been created after the revocation time.
	EXPIRED	The process shall output: The validated certificate chain	The signature validation process results in TOTAL-FAILED because there is proof that the signature has been created after the expiration date (notAfter) of the signing certificate

Main indication	Sub-indication	Associated Validation report data	Semantics
	NOT_YET_VALID		The signature validation process results in TOTAL-FAILED because there is proof that the signature was created before the issuance date (notBefore) of the signing certificate.
INDETERMINATE	SIG_CONSTRAINTS_FAILURE	The validation process shall provide: The set of constraints that have not been met by the signature.	The signature validation process results in INDETERMINATE because one or more attributes of the signature do not match the validation constraints.
	CHAIN_CONSTRAINTS_FAILURE	The validation process shall output: • The certificate chain used in the validation process. • The set of constraints that have not been met by the chain.	The signature validation process results in INDETERMINATE because the certificate chain used in the validation process does not match the validation constraints related to the certificate.
	CERTIFICATE_CHAIN_GENERAL_FAILURE	The process shall output: Additional information regarding the reason.	The signature validation process results in INDETERMINATE because the set of certificates available for chain validation produced an error for an unspecified reason.

Main indication	Sub-indication	Associated Validation report data	Semantics
	CRYPTO_CONSTRAINTS_FAILURE	The process shall output: • Identification of the material (signature, certificate) that is produced using an algorithm or key size below the required cryptographic security level. • If known, the time up to which the algorithm or key size was considered secure.	The signature validation process results in INDETERMINATE because at least one of the algorithms that have been used in material (e.g. the signature value, a certificate...) involved in validating the signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and: • this material was produced after the time up to which this algorithm/key was considered secure (if such a time is known); and • the material is not protected by a sufficiently strong time-stamp applied before the time up to which the algorithm/key was considered secure (if such a time is known).
	POLICY_PROCESSING_ERROR	The validation process shall provide additional information on the problem.	The signature validation process results in INDETERMINATE because a given formal policy file could not be processed for any reason (e.g. not accessible, not parseable, digest mismatch, etc.).
	SIGNATURE_POLICY_NOT_AVAILABLE		The signature validation process results in INDETERMINATE because the electronic document containing the details of the policy is not available.
	TIMESTAMP_ORDER_FAILURE	The validation process shall output the list of time stamps that do not respect the ordering constraints.	The signature validation process results in INDETERMINATE because some constraints on the order of signature time-stamps and/or signed data object(s) time-stamps are not respected.
	NO_SIGNING_CERTIFICATE_FOUND		The signature validation process results in INDETERMINATE because the signing certificate cannot be identified.

Main indication	Sub-indication	Associated Validation report data	Semantics
	NO_CERTIFICATE_CHAIN_FOUND		The signature validation process results in INDETERMINATE because no certificate chain has been found for the identified signing certificate.
	REVOKED_NO_POE	The validation process shall provide the following: • The certificate chain used in the validation process. • The time and the reason of revocation of the signing certificate.	The signature validation process results in INDETERMINATE because the signing certificate was revoked at the validation date/time. However, the Signature Validation Algorithm cannot ascertain that the signing time lies before or after the revocation time.
	REVOKED_CA_NO_POE	The validation process shall provide the following: • The certificate chain which includes the revoked CA certificate. • The time and the reason of revocation of the certificate.	The signature validation process results in INDETERMINATE because at least one certificate chain was found but an intermediate CA certificate is revoked.
	OUT_OF_BOUNDS_NOT_REVOKED		The signature validation process results in INDETERMINATE because the signing certificate is expired or not yet valid at the validation date/time and the Signature Validation Algorithm cannot ascertain that the signing time lies within the validity interval of the signing certificate. The certificate is known not to be revoked.

Main indication	Sub-indication	Associated Validation report data	Semantics
	OUT_OF_BOUNDS_NO_POE		The signature validation process results in INDETERMINATE because the signing certificate is expired or not yet valid at the validation date/time and the Signature Validation Algorithm cannot ascertain that the signing time lies within the validity interval of the signing certificate.
INDETERMINATE	CRYPTO_CONSTRAINTS_FAILURE_NO_POE	The process shall output: • Identification of the material (signature, certificate) that is produced using an algorithm or key size below the required cryptographic security level. If known, the time up to which the algorithm or key size was considered secure.	The signature validation process results in INDETERMINATE because at least one of the algorithms that have been used in objects (e.g. the signature value, a certificate, etc.) involved in validating the signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and there is no proof that this material was produced before the time up to which this algorithm/key was considered secure.
	NO_POE	The validation process shall identify at least the signed objects for which the POEs are missing. • The validation process should provide additional information on the problem.	The signature validation process results in INDETERMINATE because a proof of existence is missing to ascertain that a signed object has been produced before some compromising event (e.g. a broken algorithm).

Main indication	Sub-indication	Associated Validation report data	Semantics
	TRY_LATER	The validation process shall output the point of time, where the necessary revocation information is expected to become available.	The signature validation process results in INDETERMINATE because not all constraints can be fulfilled using available information. However, it may be possible to do so using additional revocation information that will be available at a later point in time.
	SIGNED_DATA_NOT_FOUND	The process should output when available: The identifier(s) (e.g. a URI) of the signed data that caused the failure.	The signature validation process results in INDETERMINATE because signed data cannot be obtained.

- Dokobit assigns an object identifier (OID) to each policy and supports two validation policies:

Validation Policy	Object Identifier
QES validation policy • Stricter validation: requires valid qualified electronic signatures and seals to pass. Qualified electronic signatures have the equivalent legal effect of handwritten signatures according to EU Regulation No 910/2014 (eIDAS). Default in Dokobit Validation Service API *Detailed validation constraints are defined in Annex A.*	1. 3.6.1.4.1.54720.1.2
AdES validation policy • Baseline validation: checks that the document hasn't been altered and provides necessary information about the legal type and validity of electronic signatures and seals according to EU Regulation No 910/2014 (eIDAS). Default in Dokobit Portal and Dokobit Gateway *Detailed validation constraints are defined in Annex B.*	1. 3.6.1.4.1.54720.1.3

- The validation service does not accept other sources of validation policy;
- The signature validation policy may not be ignored and replaced by signature validation rules according to the protocol specified in ETSI TS 119 442;
- The validation process ensures that the signature validation policy that is used corresponds to the strategy defined in the SVS policy or the terms and conditions of use of validation service;
- The strategy defined in the SVS policy or the terms and conditions of use of the SVS follows the following principles:
    - For the same input including validation policy, the validation service will return the same output;

- SVS may accept different elements as proof of existence for a signature.

4.1.3 Validation process

Dokobit validation service supports the Validation Process for Basic Signatures and the Validation Process for Signatures with Timestamp and Signatures with Long-Term Validation Data. There is no possibility to specify the process to be used by the DA for other services. When validating an instance of a signature or a seal, the Dokobit validation service proceeds as follows:

1. SVA performs the Validation Process for all signatures not depending on their level.
2. When the validation status returned by the selected validation process returned the status indication PASSED, the SVA provides the status indication TOTAL-PASSED to the DA
3. When the validation status returned by the selected validation process returned the status indication FAILED, the SVA provides the status indication TOTAL-FAILED to the DA.
4. Otherwise, the SVA provides the status indication INDETERMINATE.

Dokobit validation service supports the formats specified by the ETSI format standards:

1. ETSI EN 319 122-1 (2023-06) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
2. ETSI EN 319 132-1 (2024-07) Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
3. ETSI EN 319 142-1 (2024-01) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
4. ETSI EN 319 162-1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers

Dokobit validation service supports by best effort formats specified by the part 2 documents (additional profiles) of the respective standards mentioned above and older versions of these standards. Dokobit validation service supports by best effort other signature formats.

The following electronic signature and electronic seal formats apply in the context of the EU legislation [CID (EU) 2015/1506] and are supported by the Dokobit validation service:

1. ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile
2. ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
3. ETSI TS 103 173 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile
4. ETSI TS 103 174 V2.2.1 (2013-06) Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

The validation process in the Dokobit portal comprises the following steps:

1. The Subscriber authenticates to the Service using electronic identification means;
2. The Subscriber selects a validation policy and uploads an electronically signed document. Dokobit validation service restricts validation policy to be either QES validation policy or AdES validation policy;

3. Dokobit validation service validates the document according to ETSI EN 319 102-1 and using the selected validation policy.
4. The report is presented to the Subscriber.

The validation process in Dokobit Validation Service comprises the following steps:

1. The Subscriber authenticates to the Service using electronic identification means;
2. The Subscriber uploads or selects an electronically signed document and selects a validation policy. Dokobit validation service restricts validation policy to be either QES validation policy or AdES validation policy;
3. Dokobit validation service validates the document according to ETSI EN 319 102-1 and using the selected validation policy.
4. The report is presented to the Subscriber.

The validation process in Dokobit Gateway and Dokobit validation service API comprises the following steps:

1. The Subscriber uploads an electronically signed document and chooses the desired validation policy. Dokobit validation service restricts validation policy to be either QES validation policy or AdES validation policy;
2. Dokobit validation service validates the document according to ETSI EN 319 102-1 and using the selected validation policy.
3. The report is returned in JSON response which contains a list of signatures and a list of signature validation errors or warnings.

4.1.4 Validation constraints for electronically signed documents

Dokobit validation service validation constraints are defined explicitly in system-specific control data and by the implementation itself.

Any validation constraints not implied by the implementation originate from the signature content itself directly (included in the signed attributes) or indirectly, i.e. by reference to an external document, provided in a machine-processable form. Additional constraints could be provided by the DA to the SVA via parameters selected by the application or the user.

This additional constraint could be provided after mutual agreement between the Dokobit validation service provider and the relying party.

General Constraints

Dokobit validation service supports the following general constraints.

Constraint	Constraint value at signature validation (SVA or DA)
Maximum file size of supported documents	300MB (Dokobit Validation Service API, Dokobit Gateway), 100MB (Dokobit Portal)

X.509 Validation Constraints

Dokobit validation service supports the following X.509 validation constraints which indicate requirements for use in the certificate path validation process as specified in ETSI 119 172-1, clause A.4.2.1, table A.2 row m.

Constraint(s)	Constraint value at signature validation (SVA or DA)
(m)1. X509CertificateValidationConstraints: This set of constraints indicates requirements for use in the certificate path validation process as defined in IETF RFC 5280. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows: (m)1.1. SetOfTrustAnchors: This constraint indicates a set of acceptable trust anchors (TAs) as a constraint for the validation process.	EU TSL UA TSL
(m)1.2. CertificationPath: This constraint indicates a certification path required to be used by the SVA for validation of the signature. The certificate path is of length 'n' from the trust anchor (TA) down to the certificate used in validating a signed object (e.g. the signer's certificate or a time-stamping certificate). This constraint can include the path to be considered or indicate the need for considering the path provided in the signature if any. • (m)1.3. user-initial-policy-set: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (c) • (m)1.4. initial-policy-mapping-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (e) • (m)1.5. initial-explicit-policy: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (f) • (m)1.6. initial-any-policy-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (g) • (m)1.7. initial-permitted-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (h) • (m)1.8. initial-excluded-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (i) • (m)1.9. path-length-constraints: This constraint indicates restrictions on the number of CA certificates in a certification path. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it) • (m)1.10. policy-constraints: This constraint indicates requirements for certificate policies referenced in the certificates. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). This should also allow the ability to require a (possible set of) specific certificate policy extension value(s) in end-entity certificates (without requiring such values to appear in the certificate of authorities in the certification path).	None

Constraint(s)	Constraint value at signature validation (SVA or DA)
(m)2. RevocationConstraints: This set of constraints indicates requirements applicable when verifying the certificate validity status of the certificates during the certificate path validation process. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows: (m)2.1. RevocationCheckingConstraints: This constraint indicates requirements for checking certificate revocation. Such constraints may specify if revocation checking is required or not and if OCSP responses or CRLs have to be used. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • clrCheck: Checks shall be made against current CRLs (or Authority Revocation Lists); • ocspCheck: The revocation status shall be checked using OCSP IETF RFC 6960; • bothCheck: Both OCSP and CRL checks shall be carried out; • eitherCheck: Either OCSP or CRL checks shall be carried out; • noCheck: No check is mandated.	eitherCheck
(m)2.2. RevocationFreshnessConstraints: This constraint indicates time requirements on revocation information. The constraints may indicate the maximum accepted difference between the issuance date of the revocation status information of a certificate and the time of validation or require the SVA to only accept revocation information issued a certain time after the signature has been created.	None
(m)2.3. RevocationInfoOnExpiredCerts: This constraint mandates the signer's certificate used in validating the signature to be issued by a certification authority that keeps revocation notices for revoked certificates even after they have expired for a period exceeding a given lower bound.	None
(m)3. LoAOnTSPPractices: This constraint indicates the required LoA on the practices implemented by the TSP(s) having issued the certificates to be validated during the certificate path validation process, i.e. the certificates present in the certificate path of the signer's certificate, and optionally those present in all or some of the other certificate chain	None

1. Based on Annex C from ETSI 119 172-1: The following constraints indicate requirements on specific certificate metadata whose semantics apply in the context of the EU legislation:

a) EUQualifiedCertificateRequired: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate as defined in the applicable EU legislation; expressed as a boolean.

b) EUQualifiedCertificateSigRequired: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate for electronic signature as defined in eIDAS; expressed as a boolean.

c) EUQualifiedCertificateSealRequired: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate for electronic seal as defined in eIDAS; expressed as a boolean.

d) EUQSCDRequired: This constraint indicates that the signer's certificate used in validating the signature is required to be related to the private key which is stored in the Qualified Signature Creation Device as defined in eIDAS; expressed as a boolean.

Cryptographic Constraints

Dokobit validation service supports the following cryptographic constraints which indicate requirements on algorithms and parameters used when creating signatures or used when validating signed objects as specified in ETSI TS 119 172-1, clause A.4.2.1, table A.2 row p.

Contraint(s)	Constraint value at signature validation (SVA or DA)
(p)1. CryptographicSuitesConstraints: This constraint indicates requirements on algorithms and parameters used when creating signatures or used when validating signed objects included in the validation or augmenting process (e.g. signature, certificates, CRLs, OCSP responses, time-stamps). Typically, they will be represented by a list of entries as in table A.3.	Based on ETSI TS 119 312

Signature and Seal Elements Constraints

Dokobit validation service supports the following signature elements constraints which indicate requirements on the DTBS as specified in ETSI TS 119 172-1, clause A.4.2.1, table A.2 row b.

Contraint(s)	Constraint value at signature validation (SVA or DA)
(b)1. ConstraintOnDTBS: This constraint indicates requirements on the type of data to be signed by the signer.	None

Contraint(s)	Constraint value at signature validation (SVA or DA)
(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: This set of constraints indicates the required content-related information elements under the form of signed or unsigned qualifying properties that are mandated to be present in the signature. This includes: (b)2.1 MandatedSignedQProperties-DataObjectFormat to require a specific format for the content being signed by the signer. (b)2.2 MandatedSignedQProperties-content-hints to require specific information that describes the innermost signed content of a multi-layer message where one content is encapsulated in another for the content being signed by the signer. (b)2.3 MandatedSignedQProperties-content-reference to require the incorporation of information on the way to link request and reply messages in an exchange between two parties, or the way such link has to be done, etc. (b)2.4 MandatedSignedQProperties-content-identifier to require the presence of, and optionally a specific value for, an identifier that can be used later on in the sig	None
(b)3. DOTBSAsAWholeOrInParts: This constraint indicates whether the whole data or only certain part(s) of it have to be signed. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • whole: the whole data has to be signed; • parts: only certain part(s) of the data have to be signed. In this case, additional information should be used to express which parts have to be signed.	None

4.2 Signature validation protocol requirements

The communication channel between the client and the validation service transports the validation requests for the electronic signature in one direction and returns the response. It can be either synchronous or asynchronous. The validation protocol corresponds to ETSI TS 119 442.

Dokobit validation services are available at these means:

- as a REST API integration (Dokobit Gateway or Dokobit Validation Service API);
- as a Web Application with a User Interface (Dokobit portal or Dokobit Validation Service).

4.3 Interfaces

4.3.1 Communication channel

The communication channel between the client and the SVSP is secured by using a reliably protected channel under HTTPS protocol and using TLS encryption with QWAC certificate. SVSP guarantees that it can establish a secure channel with the client and keep the confidentiality of data.

Dokobit portal requires a client to authenticate to the service using electronic identification means and only then can the client access the validation service, therefore, it ensures that uploaded information is accessible only for a particular client.

Dokobit Gateway and Dokobit Validation Service API require the user to authorise using an authorisation access token, which ensures that uploaded information is accessible only to a particular client. IP protection can be used as well.

4.3.2 SVSP - Other Trust Service Providers

The signature verification status and the signature validation report may be affected by the practices, policies and agreements for compliance with other service providers that are outside the control of the SVSP. Other trust service providers include time-stamping authorities, CRL and OCSP providers, and other validation service providers. SVSP provided signature verification status and the signature validation report is only valid at the actual validation time.

The communication channel between the SVSP and other TSP is outside the scope of this document.

4.4 Signature validation report requirements

SVSP provides three types of validation reports:

1. Simple Validation Report - It provides necessary information regarding the Signer's identity and the status indication per validated signature, including sub-indication.
2. Detailed Validation Report - It provides a report on each of the validation constraints that is processed including any validation constraints that have been applied implicitly by the implementation.
3. Machine-readable Validation Report - It provides a detailed validation report in machine-readable XML format.

All validation reports provided by SVSP shall be sealed using the Advanced Electronic Seal with a Qualified Certificate.

Qualified Certificate for Seal is issued by Qualified Trust Service Provider - SK ID Solutions - in accordance with SK ID Solutions Certification Practice Statement for KLASS3-SK - SK-CPS-KLASS3-v8.0, which is available at *https://www.sk.ee/upload/files/SK-CPS-KLASS3-EN-v8_0_20190815.pdf*.

Seal certificate details:

cn=Dokobit Qualified Validation Service

o=Dokobit UAB

c=LT

l=Vilnius

st=Vilnius

serialNumber=301549834

2.5.4.97=NTRLT-301549834

Issuer details:

cn=KLASS3-SK 2016

2.5.4.97=NTREE-10747013

ou=Sertifitseerimisteenused

o=AS Sertifitseerimiskeskus

c=EE

5 Annex A

Common signature validation constraints for QES Validation Policy (1.3.6.1.4.1.54720.1.2):

Constraint	Indication
Container constraints	
Acceptable container types: ASiC-S ASiC-E	FAIL
MimeType file is present	FAIL
Acceptable MimeType file content: application/vnd.etsi.asic-s+zip application/vnd.etsi.asic-e+zip	WARN
Manifest file is present	FAIL
All files are signed	WARN
Signature constraints	
Acceptable policies: ANY_POLICY NO_POLICY	FAIL
Policy is available	FAIL
Policy hash matches	FAIL
Reference data exists	FAIL
Reference data is intact	FAIL
Manifest entry object exists	WARN
Signature is intact	FAIL

Prospective certificate chain	FAIL
Signing certificate recognition	FAIL
Signing certificate signature	FAIL
Signing certificate qualification	FAIL
Signing certificate is supported by QSCD	FAIL
Signing certificate is not expired	WARN
Signing certificate authority info access is present	WARN
Signing certificate revocation info access is present	WARN
Signing certificate revocation data is available	FAIL
Signing certificate revocation data next update is present	WARN
Signing certificate revocation data freshness	WARN
Signing certificate key usage contains “nonRepudiation“	WARN
Signing certificate serial number is present	WARN
Signing certificate is not revoked	FAIL
Signing certificate is not on hold	FAIL
Signing certificate is not self-signed	WARN
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	WARN
Certification authority certificate revocation data is available	FAIL
Certification authority certificate revocation data next update is present	WARN
Certification authority certificate revocation data freshness	WARN

Certification authority certificate is not revoked	FAIL
Certification authority certificate is not on hold	FAIL
Signed attributes contain signing certificate	FAIL
Signed attributes contain signing certificate digest	FAIL
Signing certificate digest in signed attributes matches	FAIL
Issuer serial digest in signed attributes matches	WARN
Signed attributes contain signing time	FAIL
Signed attributes contain message digest or signed properties	FAIL
Elements that might change the visual content of the signed document were detected	WARN
Timestamp constraints	
Revocation time is against best signature time	FAIL
Best signature time is before issuance date of signing certificate policy	FAIL
Coherence	WARN
Reference data exists	FAIL
Reference data is intact	FAIL
Signature is intact	FAIL
Prospective certificate chain	FAIL
Signing certificate recognition	FAIL
Signing certificate signature	FAIL
Signing certificate is not expired	WARN

Signing certificate revocation data is available	FAIL
Signing certificate revocation data next update is present	WARN
Signing certificate revocation data freshness	WARN
Signing certificate key usage contains “timeStamping“	WARN
Signing certificate is not revoked	FAIL
Signing certificate is not on hold	FAIL
Signing certificate is not self-signed	WARN
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	WARN
Certification authority certificate revocation data is available	WARN
Certification authority certificate revocation data next update is present	WARN
Certification authority certificate revocation data freshness	WARN
Certification authority certificate is not revoked	FAIL
Certification authority certificate is not on hold	FAIL
Revocation constraints	
Reference data exists	FAIL
Reference data is intact	FAIL
Signature is intact	FAIL
Prospective certificate chain	WARN
Signing certificate recognition	FAIL
Signing certificate signature	FAIL

Signing certificate is not expired	WARN
Signing certificate revocation data is available	IGNORE
Signing certificate revocation data next update is present	IGNORE
Signing certificate revocation data freshness	IGNORE
Signing certificate is not revoked	IGNORE
Signing certificate is not on hold	IGNORE
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	IGNORE
Certification authority certificate revocation data is available	IGNORE
Certification authority certificate revocation data next update is present	IGNORE
Certification authority certificate revocation data freshness	IGNORE
Certification authority certificate is not revoked	IGNORE
Certification authority certificate is not on hold	IGNORE
Trusted list constraints	
Trusted list freshness	WARN
Trusted list is not expired	WARN
Trusted list is well signed	FAIL
Trusted list version 5	FAIL
Trusted list consistency	FAIL
Cryptographic constraints	

Acceptable encryption algorithms: RSA - (minimum key size 1024) DSA - (minimum key size 160) ECDSA - (minimum key size 160) PLAIN-ECDSA - (minimum key size 160)	FAIL
Acceptable digest algorithms: SHA1, SHA224, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD160, WHIRLPOOL	FAIL
Algorithm expiration date: SHA1 - 2009 SHA224 - 2023 SHA256 - 2026 SHA384 - 2026 SHA512 - 2026 SHA3-224 - 2026 SHA3-256 - 2026 SHA3-384 - 2026 SHA3-512 - 2026 RIPEMD160 - 2011 WHIRLPOOL - 2015 DSA 160 - 2013 DSA 192 - 2013 DSA 224 - 2023 DSA 256 - 2026 RSA 1024 - 2009 RSA 1536 - 2016 RSA 2048 - 2023 RSA 3072 - 2026 RSA 4096 - 2026 ECDSA 160 - 2013 ECDSA 192 - 2013 ECDSA 224 - 2016 ECDSA 256 - 2026 ECDSA 384 - 2026 ECDSA 512 - 2026 PLAIN-ECDSA 160 - 2013 PLAIN-ECDSA 192 - 2013 PLAIN-ECDSA 224 - 2016 PLAIN-ECDSA 256 - 2026 PLAIN-ECDSA 384 - 2026 PLAIN-ECDSA 512 - 2026	FAIL

- *FAIL - if the constraint is not met, validation shows an error*
- *WARN - if the constraint is not met, validation shows a warning*
- *IGNORE - constraint is ignored*

6 Annex B

Common signature validation constraints for AdES Validation Policy (1.3.6.1.4.1.54720.1.3):

Constraint	Indication
Container constraints	
Acceptable container types: ASiC-S ASiC-E	FAIL
MimeType file is present	FAIL
Acceptable MimeType file content: application/vnd.etsi.asic-s+zip application/vnd.etsi.asic-e+zip	WARN
Manifest file is present	FAIL
All files are signed	WARN
Signature constraints	
Acceptable policies: ANY_POLICY NO_POLICY	FAIL
Policy is available	FAIL
Policy hash matches	FAIL
Reference data exists	FAIL
Reference data is intact	FAIL
Manifest entry object exists	WARN
Signature is intact	FAIL

Prospective certificate chain	FAIL
Signing certificate recognition	FAIL
Signing certificate signature	FAIL
Signing certificate qualification	IGNORE
Signing certificate is supported by QSCD	IGNORE
Signing certificate is not expired	FAIL
Signing certificate authority info access is present	WARN
Signing certificate revocation info access is present	WARN
Signing certificate revocation data is available	FAIL
Signing certificate revocation data next update is present	WARN
Signing certificate revocation data freshness	WARN
Signing certificate key usage contains “nonRepudiation“	WARN
Signing certificate serial number is present	WARN
Signing certificate is not revoked	FAIL
Signing certificate is not on hold	FAIL
Signing certificate is not self-signed	WARN
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	WARN
Certification authority certificate revocation data is available	FAIL
Certification authority certificate revocation data next update is present	WARN
Certification authority certificate revocation data freshness	WARN

Certification authority certificate is not revoked	FAIL
Certification authority certificate is not on hold	FAIL
Signed attributes contain signing certificate	FAIL
Signed attributes contain signing certificate digest	FAIL
Signing certificate digest in signed attributes matches	FAIL
Issuer serial digest in signed attributes matches	WARN
Signed attributes contain signing time	FAIL
Signed attributes contain message digest or signed properties	FAIL
Elements that might change the visual content of the signed document were detected	WARN
Timestamp constraints	
Revocation time is against best signature time	FAIL
Best signature time is before issuance date of signing certificate policy	FAIL
Coherence	WARN
Reference data exists	FAIL
Reference data is intact	FAIL
Signature is intact	FAIL
Prospective certificate chain	FAIL
Signing certificate recognition	FAIL
Signing certificate signature	FAIL
Signing certificate is not expired	WARN

Signing certificate revocation data is available	FAIL
Signing certificate revocation data next update is present	WARN
Signing certificate revocation data freshness	WARN
Signing certificate key usage contains “timeStamping“	WARN
Signing certificate is not revoked	FAIL
Signing certificate is not on hold	FAIL
Signing certificate is not self-signed	WARN
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	WARN
Certification authority certificate revocation data is available	WARN
Certification authority certificate revocation data next update is present	WARN
Certification authority certificate revocation data freshness	WARN
Certification authority certificate is not revoked	FAIL
Certification authority certificate is not on hold	FAIL
Revocation constraints	
Reference data exists	FAIL
Reference data is intact	FAIL
Signature is intact	FAIL
Prospective certificate chain	WARN
Signing certificate recognition	FAIL
Signing certificate signature	FAIL

Signing certificate is not expired	WARN
Signing certificate revocation data is available	IGNORE
Signing certificate revocation data next update is present	IGNORE
Signing certificate revocation data freshness	IGNORE
Signing certificate is not revoked	IGNORE
Signing certificate is not on hold	IGNORE
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	IGNORE
Certification authority certificate revocation data is available	IGNORE
Certification authority certificate revocation data next update is present	IGNORE
Certification authority certificate revocation data freshness	IGNORE
Certification authority certificate is not revoked	IGNORE
Certification authority certificate is not on hold	IGNORE
Trusted list constraints	
Trusted list freshness	WARN
Trusted list is not expired	WARN
Trusted list is well-signed	FAIL
Trusted list version 5	FAIL
Trusted list consistency	FAIL
Cryptographic constraints	

Acceptable encryption algorithms: RSA - (minimum key size 1024) DSA - (minimum key size 160) ECDSA - (minimum key size 160) PLAIN-ECDSA - (minimum key size 160)	FAIL
Acceptable digest algorithms: SHA1, SHA224, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD160, WHIRLPOOL	FAIL
Algorithm expiration date: SHA1 - 2009 SHA224 - 2023 SHA256 - 2026 SHA384 - 2026 SHA512 - 2026 SHA3-224 - 2026 SHA3-256 - 2026 SHA3-384 - 2026 SHA3-512 - 2026 RIPEMD160 - 2011 WHIRLPOOL - 2015 DSA 160 - 2013 DSA 192 - 2013 DSA 224 - 2023 DSA 256 - 2026 RSA 1024 - 2009 RSA 1536 - 2016 RSA 2048 - 2023 RSA 3072 - 2026 RSA 4096 - 2026 ECDSA 160 - 2013 ECDSA 192 - 2013 ECDSA 224 - 2016 ECDSA 256 - 2026 ECDSA 384 - 2026 ECDSA 512 - 2026 PLAIN-ECDSA 160 - 2013 PLAIN-ECDSA 192 - 2013 PLAIN-ECDSA 224 - 2016 PLAIN-ECDSA 256 - 2026 PLAIN-ECDSA 384 - 2026 PLAIN-ECDSA 512 - 2026	FAIL

- *FAIL - if the constraint is not met, validation shows an error*
- *WARN - if the constraint is not met, validation shows a warning*
- *IGNORE - constraint is ignored*