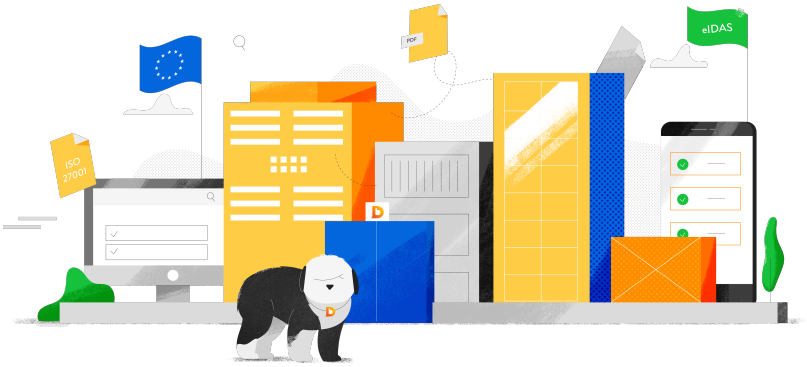


Qualified Signature and Seal Validation Service Practice Statement and Policy v1.10

Document Number: DKB-VSP-06122019 v1.10

Unique object ID (OID): 1.3.6.1.4.1.54720.1.1

Effective from 2021-08-02

Table of Contents

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

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** 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;
- 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 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 April21, 2018
    - The Description of the Procedure for Reporting Breaches of the Security and/or Integrity of Trust Services approved by Order No. 1V-594 of the Director of the Communications Regulatory Authority on 4 June 2019
- European standard *ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI)*
    - General Policy Requirements for Trust Service Providers and other related requirements.

The structure of this document is compliant to the *Annex A of ETSI TS 119 441 V1.1.1 (2018-08)*.

2.1.1 TSP identification

Dokobit, UAB

Company code 301549834

Paupio g. 46, 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 signature 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

2.2 Signature validation service components

2.2.1 SVS actors

Signature Validation Client

(SVC)

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

Driving Application (DA)

- Application which provides signature validation functionality to Signature Validation Client.

Signature Validation Service Protocol (SVP)

- Secure communication channel for exchanging information with 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)

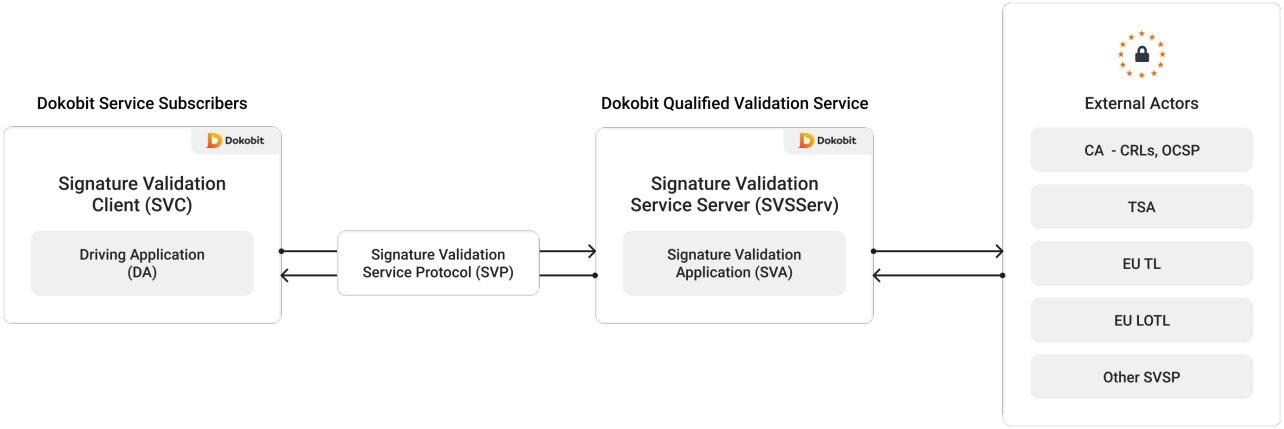
- A software component that is responsible for signature validation, which implements the validation algorithm and creates a signature validation report.

External Actors

- Other trust sources - Certification Authorities, Time-stamping authorities, European Trusted List providers, European Commission providing the list of Trusted Lists which are called to fulfil its 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.
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).
Information Security Management System	ISMS	Dokobit's certified Information Security Management System according to ISO/IEC 27001:2013.
Trust Service Provider	TSP	An entity which provides Trust Service.
Qualified Trust Service Provider	QTSP	An entity which provides one or more Qualified Trust Services and is granted the 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.

Name	Abbreviation	Definition
Dokobit Signature Validation Practice Statement	Dokobit PS	A statement of the practices that Dokobit employs in providing Trust Service.
Signature Validation Service	SVS	Trust Service for Signature and / or Seal Validation.
Relying Party		A natural or legal person that relies on Trust Service.
Subscriber		A legal or natural person bound by an agreement with Dokobit to any Subscriber obligations.
Certification Authority	CA	Qualified Trust Service Provider that issues 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

2.4 Policies and Practices

2.4.1 Organization administrating the TSP documentation

This document is administered by Dokobit.

Dokobit, UAB

Company code 301549834

Paupio g. 46, 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 Compliance Manager of Dokobit.

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

2.4.3 TSP documentation applicability

Signature Validation Service Practice statement

Dokobit is responsible for the management of Dokobit Validation Service Practice Statement. This document shall be approved by the Management Board and made publicly at Dokobit Compliance website (*https://www.dokobit.com/compliance*).

Dokobit shall notify 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 Supervisory body about the planned termination of the qualified trust service no less than 3 months prior to the the termination of qualified trust service.

Notification to Supervisory Body shall be sent without undue delay and not later than 3 workdays after any changes in Dokobit Validation Service Practice Statement.
Subscribers and Relying parties shall only take into account the effective version of Dokobit PS as of the time of using the services provided by Dokobit. Dokobit PS along with enforcement dates is published no less than 30 days prior to taking effect.

Information security policy

Dokobit has implemented an Information Security Management System (ISMS) according to ISO/IEC-27001:2013 standard. Dokobit has achieved certification of ISMS according to ISO/IEC-27001:2013 standard with the certification scope of “Cloud-based services for e-signing, e-sealing, e-identification, validation of e-signature and e-seal, and related software development, delivery and support.”

Dokobit has implemented all necessary controls required by eIDAS and GDPR regulations and corresponding standards (i.e. ETSI EN 319 401) into ISMS.

Dokobit Chief Executive Officer approves policies and practices related to information security.

Terms of Service

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

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 the 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 the 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.

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

3 Trust Service Management And Operation

Dokobit has implemented an Information Security Management System according to ISO/IEC 27001:2013 standard and has achieved *ISO/IEC 27001:2013 certification* by an accredited international certification body. Qualified Signature and Seal Validation Services are within the scope of this certification. The paragraphs below summarize management and operations of trust service, including security controls applied.

3.1 Internal organization

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. Dokobit ensures that all requirements defined in ISO27001:2013 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 Organization 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 organization reliability measures upon special legitimate request from concerning party.

3.1.2 Segregation of duties

Implemented and certified Information Security Management System according to ISO/IEC 27001:2013 ensures that segregation of duties is verified and maintained. More specifically: Information security manager (ISM) and internal auditor roles are separated. More specifically:

A.6.1.2	Segregation of duties	ISM and Internal Auditor roles are separated. Also, the Management group is established to deal with major issues, including issues in information security. ISM is a part of the Management group. Four eyes principle is ensured in vital areas: • Secure development and code reviews • Software deployments

3.2 Human resources

Implemented and certified Information Security Management System according to ISO/IEC 27001:2013 ensures that Dokobit has implemented all necessary controls for secure operations. The employees and contractors receive adequate training and have all the necessary experience for carrying out the duties specified in employment or contractor's agreements as defined in Dokobit HR Management Policy. More specifically:

A.7.1	Prior to employment	
A.7.1.1	Screening	HR Management Policy is a part of ISMS. If defines recruitment, on-boarding and employment termination processes. Pre-employment checks and vetting, including checks on criminal convictions as required for Qualified Trust Service providers, employment history and references are part of Dokobit recruitment process.
A.7.1.2	Terms and conditions of employment	Every employee signs a standardised form of an employment contract and confidentiality agreement before employment and actual work-related activities. In addition, an employee is getting familiarised with the list of business secrets which is approved by organisation's management board and all the information and data that fit into the defined categories need to be kept as a business secret and protected.
A.7.2	During employment	
A.7.2.1	Management responsibilities	Management governs and supports ISMS activities and employees are one of the essential parts of ISMS. Governing process and management responsibilities are described in Information security policy and management practice document.
A.7.2.2	Information security awareness, education and training	Training and internal awareness activities are essential for personnel to understand the importance of information security management and their own contribution to ISMS, accept policies and plans, and understand the consequences of breaching the information security rules. As a result, training and awareness plan is prepared and coordinated by ISM. Its execution results in associated tangible records. In addition, secure development practices, including associated awareness are provided in Secure Development Policy.

A.7.2.3	Disciplinary process	According to HR Management Policy, disciplinary actions are part of: • Labour Code of the Republic of Lithuania; • Employment contract; • Special NDA clauses signed by an employee. This policy provides a procedure for the disciplinary process, which might result in the termination of an employment agreement and fines defined in NDA.
A.7.3	Termination and change of employment	
A.7.3.1	Termination or change of employment responsibilities	According to the NDAs with employees, confidentiality statements remain valid after the termination of employment. Employment termination procedure and necessary steps related to it, like disabling access rights, are described in the HR Management Policy and Access Control Policy. In addition, a review of access rights should be performed as per Access Control Policy when changes in employment responsibilities occur.

3.3 Asset management

3.3.1 General requirements

Dokobit maintains up-to-date lists of assets, incl. information 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. This is a part of Dokobit certified ISMS - i.e. Dokobit Acceptable Use Policy, Dokobit Information Classification Policy and Dokobit Risk Management Methodology. More specifically:

A.8.1	Responsibility for assets	
A.8.1.1	Inventory of assets	Dokobit maintains up-to-date lists of all assets (both virtual and physical) and their owners. Organisation's risk assessment is aligned with the identification of assets and threats are identified as related to assets using elaborate mapping.
A.8.1.2	Ownership of assets	Dokobit maintains up-to-date lists of all assets (both virtual and physical) and their owners. Table “List of assets” represents asset owners.

A.8.1.3	Acceptable use of assets	Acceptable Use Policy defines clear rules for the use of information systems and other information assets at Dokobit. It also defines responsibilities, prohibited activities, taking assets off-site, returns of assets, backups, internet use within assets, mobile computing, teleworking.
A.8.1.4	Return of assets	Dokobit ensures that all the equipment, software and information in electronic and paper form is returned, where applicable. Return of assets is defined in NDAs (as required per HR Management Policy), Acceptable Use Policy, Supplier agreements (as required per Supplier Security Policy).

3.3.2 Media handling

Media containing sensitive information is handled securely and in accordance with ISMS Dokobit Information Classification Policy and Dokobit Operating Procedures for ICT. More specifically:

A.8.3	Media handling	
A.8.3.1	Management of removable media	Information Classification Policy defines how to handle information in printed, electronic, electronic within information systems, and email formats, including removable media (and storage). It includes access, usage of passwords and encryption.
A.8.3.2	Disposal of media	Operating Procedures for ICT document provides controls for disposal and destruction of equipment and media. In general, all equipment containing storage media (e.g. computers, mobile phones, etc.) must be wiped-out before it is reused or media destroyed before it is disposed of.
A.8.3.3	Physical media transfer	Information Classification Policy defines technical security controls for securing information in media, including for transfer, depends on the classification level. Operating Procedures for ICT document provides requirement to wipe-out any kind of media before it is reused

3.4 Access control

Dokobit Access Control Policy which is a part of Dokobit certified ISMS ensures that system access shall be limited to authorized individuals and all necessary controls for secure access control are implemented. More specifically:

A.9	Access control	
A.9.1	Business requirements of access control	
A.9.1.1	Access control policy	The basic principle is that access to all systems, networks, services and information is forbidden (“denied by default”), unless expressly permitted (“need to know”) to individual users or groups of users. 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.
A.9.1.2	Access to networks and network services	The basic principle is that access to all systems, networks, services and information is forbidden (“denied by default”), unless expressly permitted (“need to know”) to individual users or groups of users. Remote access is supported in an encrypted manner only (Operating Procedures for ICT) and is a subject to Acceptable Use Policy at Dokobit.
A.9.2	User access management	
A.9.2.1	User registration and de-registration	Dokobit Access Control Policy provides a framework for registering a user in the corporate directory, internal network and information systems. Also, recommended technical (security) parameters supplement user registration process. Access control policy also provides user de-registration process, including requirements for accounts removal.
A.9.2.2	User access provisioning	The basic principle is that access to all systems, networks, services and information is forbidden (“denied by default”), unless expressly permitted (“need to know”) to individual users or groups of users. Remote access is supported in an encrypted manner only (Operating Procedures for ICT) and is a subject to Acceptable Use Policy at Dokobit. Requirements for corporate account security settings are also located in this document.
A.9.2.3	Management of privileged access rights	According to Dokobit Access Control Policy, privileges for each system (asset) may be granted by their respective owners only or ISM.
A.9.2.4	Management of secret authentication information of users	Dokobit Acceptable Use Policy provides comprehensive requirements for users to manage and use secret authentication information. It enforces best industry practices, like enforced 2F.
A.9.2.5	Review of user access rights	Regular review of access rights is defined in Access Control Policy.

A.9	Access control	
A.9.2.6	Removal or adjustment of access rights	Access rights are being removed or adjusted by following Access Control Policy. Despite a timely change of access rights upon business requests, responsible manager guarantees and ensures that access rights for every system/sub-system/component are reviewed at least once per year.
A.9.3	User responsibilities	
A.9.3.1	Use of secret authentication information	Dokobit Acceptable Use Policy provides comprehensive requirements for users to manage and use secret authentication information. It enforces best industry practices, like using encrypted password management tools.
A.9.4	System and application access control	
A.9.4.1	Information access restriction	Information Classification Policy defines information access restriction and provision procedures. In Addition, Access Control Policy defines the basic principle that access to all systems, networks, services and information is forbidden (“denied by default”), unless expressly permitted (“need to know”) to individual users or groups of users.
A.9.4.2	Secure log-on procedures	(Electronic) access provision rules in Access Control Policy requires that access to the internal, external or third party service/application should be provided by using federated corporate account authentication service. It also includes industry best practices like enforcement of 2F.
A.9.4.3	Password management system	Detailed requirements for corporate account security settings are listed in the Access Control Policy, which reflects industry best practices.
A.9.4.4	Use of privileged utility programs	There is a limitation in Acceptable Use Policy that users must not take part in activities which may be used to bypass information system security controls.
A.9.4.5	Access control to software source code	The program source code is intellectual property and is accessible on a basis need-to-know only. Information Classification Policy defines authorised persons and access restrictions to business secrets (program source code is a part of business secrets). Physically source code is stored in the Source Code Versioning system, where ISM provides key-based access to required sources.

3.5 Cryptographic controls

Dokobit Policy on the use of cryptographic controls which is a part of Dokobit certified ISMS ensures the use of secure cryptographic algorithms, keys sizes and cryptographic devices in the provision of all Dokobit Services.

A.10	Cryptography	
A.10.1	Cryptographic controls	
A.10.1.1	Policy on the use of cryptographic controls	Policy on the Use of Cryptographic Controls defines rules (regulation) for the use of cryptographic controls, as well as the rules for the use of cryptographic keys, in order to protect the confidentiality, integrity, authenticity and non-repudiation of information.
A.10.1.2	Key management	Policy on the Use of Cryptographic Controls defines the management of keys, including their distribution practices.

3.6 Physical and environmental security

Dokobit certified ISMS covers this section via Dokobit Supplier Security Policy, Dokobit Procedures for working in secure areas and Dokobit Operating Procedures for ICT. More specifically:

A.11	Physical and environmental security	
A.11.1	Secure areas	
A.11.1.1	Physical security perimeter	Physical security perimeter for Dokobit is defined in the Access Control Policy. Specific, vital to physical security zones, named as “secure areas” are described in the document Procedures for Working in Secure Areas.
A.11.1.2	Physical entry controls	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 Procedures for Working in Secure Areas that depend on facility vitality. For example, access to secure areas is “denied by default” (e.g. locked) except permitted by the responsible group.

A.11	Physical and environmental security	
A.11.1.3	Securing offices, rooms and facilities	Security controls for office premises are evaluated during the risk assessment and necessary actions are taken when higher than tolerable risks area being evaluated. Security controls are described in Access Control Policy and Procedures for Working in Secure Areas.
A.11.1.4	Protecting against external and environmental threats	Security controls for office premises are evaluated during the risk assessment and necessary actions are taken when higher than tolerable risks area being evaluated. However, due to the nature of Dokobit activities and the use of public cloud IaaS providers, it is not reliant on one or few fixed physical locations.
A.11.1.5	Working in secure areas	Rules for working in secure areas are described in the document Procedures for Working in Secure Areas. It defines a list of such areas, entry controls, access procedures, including for visitors, and list of prohibited activities.
A.11.1.6	Delivery and loading areas	Public access areas including delivery and loading zone (entrance to the office building) are controlled by the office building's security guard.
A.11.2	Equipment	
A.11.2.1	Equipment siting and protection	Dokobit services rely on major cloud providers that were objectively evaluated and selected by using criteria defined in internal Supplier Security Policy (applied to IaaS and SaaS). Cloud providers' declarations on various relevant certifications ensure the protection of equipment and data in cloud data centres. In addition, relevant in-house equipment is located in secure areas only. The document on Procedures for Working in Secure Areas describes a list of secure areas and associated protection controls and procedures. Secure areas is a subject of Dokobit ISO27001 scope and certification, and are periodically assessed by a selected certification body.
A.11.2.2	Supporting utilities	Dokobit services rely on major cloud providers that were objectively evaluated and selected by using criteria defined in internal Supplier Security Policy (applied to IaaS and SaaS). Cloud providers' declarations on various relevant certifications ensure supporting utilities in cloud data centres. For in-house equipment, supporting utilities are subject to risks identified during risk assessment activities and implemented as a risk treatment activities.
A.11.2.3	Cabling security	Security controls for cabling security are evaluated during the risk assessment and necessary actions are taken when higher than tolerable risks are identified.

A.11	Physical and environmental security	
A.11.2.4	Equipment maintenance	Acceptable Use Policy describes that equipment maintenance shall be done in accordance with the manufacturer's instructions. Also, it enforces specific requirements associated with maintenance, e.g. patching.
A.11.2.5	Removal of assets	Operating Procedures for ICT document describes requirements for wiping-out (in case of asset removal for re-usage) and destruction of media (which is a part of assets)(in case of disposal)
A.11.2.6	Security of equipment and assets off-premises	Dokobit Acceptable Use Policy defines the procedure of how assets may be taken off-site. It also describes rules on how assets should be handled and secured outside the office premises.
A.11.2.7	Secure disposal or reuse of equipment	Operating Procedures for ICT document provides controls for disposal and destruction of equipment and media. In general, all equipment containing storage media (e.g. computers, mobile phones, etc.) must be wiped-out before it is reused or media destroyed before it is disposed of.
A.11.2.8	Unattended user equipment	Acceptable Use Policy defines Clear Desk and Clear Screen Policy. BYOD Policy defines how the user's personal equipment might be used for work purposes. In addition, Dokobit enforces management of confidential information, including specific controls for "data in use", "data in transit", and "data at rest" states.
A.11.2.9	Clear desk and clear screen policy	Acceptable Use Policy defines clear desk and clear screen requirements. It includes actionable controls, like no sensitive documents on the desk while the user is absent. Also, it enforces locking down computer screens before leaving the computer workplace.

3.7 Operation security

Dokobit certified ISMS covers this section via Dokobit Operating Procedures for ICT, Dokobit Secure Development Policy, Dokobit Supplier Security Policy, Dokobit Incident Management Procedure, Dokobit Acceptable Use Policy, Dokobit BYOD Policy and Dokobit Personal Data Protection policy. More specifically:

A.12	Operations security	
A.12.1	Operational procedures and responsibilities	

A.12	Operations security	
A.12.1.1	Documented operating procedures	Dokobit document Operating Procedures for ICT defines necessary operating procedures. It includes change management, technical vulnerability management, backup, network security management, disposal and destruction of equipment and media, and other related relevant procedures.
A.12.1.2	Change management	Change management procedure is defined in the document Operating Procedures for ICT. The essence of it is that every change must have an owner, be traceable, documented (in tracking system) and tested, and confirmed before go-live mode. In order to ensure the proper functioning of the validation service, Dokobit runs positive and negative tests (such as XAdES, PAdES, CAdES signature validation tests, functionality logic, user-interface, security tests etc) after each change for validating service functionality.
A.12.1.3	Capacity management	Capacity is ensured and managed through service/application logging and monitoring (which is a part of IaaS/SaaS selection criteria defines in Supplier Security Policy). More details are provided in: • Operating Procedures for ICT • Secure Development Policy These requirements resulted in sophisticated internal services' monitoring system used at Dokobit.
A.12.1.4	Separation of development, testing and operational environments	Secure Development Policy defines the requirements for separation and maintenance of separate development, testing, and production environments. These requirements are part of secure engineering principles that are implemented at Dokobit.
A.12.2	Protection from malware	

A.12	Operations security	
A.12.2.1	Controls against malware	Dokobit employs a layered security approach for protection against malware. Acceptable Use Policy and BYOD Policy describe anti-malware protection mechanisms for endpoints (e.g. antivirus; least possible privilege needed to perform activities), supported by the list of prohibited activities (e.g. it is forbidden to disable permanently antivirus in endpoints; install illegal software or software from not trusted sources). At the network layer, Operating Procedures for ICT regulate network security (e.g. "Deny-by-default" all network ports, except "need-to-use"). At the applications/services layer, Secure Development Policy provides best practices and key requirements for secure software development that allows developing more resilient software against malicious activities, including malware (e.g. requirement to use OWASP guidelines; specific checklist for vital components like API, security headers and configurations, logging, etc.). In addition, Vulnerability Disclosure Policy enables community-based ("white and grey hats") vulnerabilities identification in Dokobit assets that, together with proactive technical vulnerability management practices described in Operating Procedures for ICT, eliminate possible root causes for malicious activities, including malware and its persistence.
A.12.3	Backup	
A.12.3.1	Information backup	Operating Procedures for ICT defines requirements and routine activities towards information backups. Backup copies are ensured for all Dokobit online products and services provided for clients. The backup process is automated and 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.
A.12.4	Logging and monitoring	
A.12.4.1	Event logging	Secure Development Policy defines rules for the secure development of software and systems. It provides comprehensive guidelines for service/application logging and monitoring.
A.12.4.2	Protection of log information	Logs separation from service/application environment (or via replication mechanisms) must be ensured as per Secure Development Policy requirements.
A.12.4.3	Administrator and operator logs	Logs separation from service/application environment (or via replication mechanisms) must be ensured as per Secure Development Policy requirements. In addition, Dokobit owns internal log management system which enables timely and predictive maintenance of services provided to its clients.

A.12	Operations security	
A.12.4.4	Clock synchronization	Clocks of systems are synchronised by the IaaS vendor. Synchronisation settings are subject to check as part of Secure Development Policy requirements. In addition to this, Qualified Timestamping Authority is used.
A.12.5	Control of operational software	
A.12.5.1	Installation of software on operational systems	In order to install any software in information systems, change management has to be applied which is described in document Operating Procedures for ICT. The essence of change management is that every change must have an owner, be traceable, documented (in tracking system) and tested and confirmed before go-live mode. For endpoints, it is documented in Acceptable Use and BYOD Policies.
A.12.6	Technical vulnerability management	
A.12.6.1	Management of technical vulnerabilities	Vulnerability Disclosure Policy enables community-based (“white and grey hats”) vulnerabilities identification in Dokobit assets, which, together with proactive technical vulnerability management practices described in Operating Procedures for ICT, provides a comprehensive framework for managing technical vulnerabilities. The owner of these activities is ISM.
A.12.6.2	Restrictions on software installation	Acceptable Use Policy, as well as BYOD, defines that it is forbidden to install illegal software or software from untrusted sources on a computer. Software installation in servers is subject to Change Management Procedure, which is described in Operating Procedures for ICT document.
A.12.7	Information systems audit considerations	
A.12.7.1	Information systems audit controls	Dokobit holds a layered approach for information system audit controls. During development and deployment, it is ensured through code review, test and validation, which is described in the Secure Development Policy. Many controls are ensured throughout services/ application logging and monitoring. Implemented controls are also being evaluated during risk assessment exercises that are performed annually and on an ad-hoc basis, triggered when major changes occur. In addition, these controls are subject for evaluation in the “lessons learned” context defined in the Incident Management Procedure. For specific cases, internal audit can be executed to evaluate the effectiveness of information system audit controls.

3.8 Network security

Dokobit certified ISMS covers this section via Dokobit Operating Procedures, Dokobit Acceptable Use Policy.

More specifically:

A.13.1	Network security management	
A.13.1.1	Network controls	ISM is responsible for managing and controlling security in company networks, including wireless and internal IaaS environments. Security controls for the network are described in the Operating Procedures for ICT.
A.13.1.2	Security of network services	ISM is responsible for managing and controlling security in company networks, including wireless and internal IaaS environments. Security controls for the network are described in the Operating Procedures for ICT. The principle “deny-by-default” all network ports, except if “need-to-use” is implemented across.
A.13.1.3	Segregation in networks	ISM is responsible for managing and controlling security in company networks, including wireless and internal IaaS environments. Security controls for the network are described in the Operating Procedures for ICT. It emphasises segregation in networks. And as a result, production (IaaS), backup and office dev/test) environments are segregated as different network layers.

3.9 Incident management

This section is covered by Dokobit certified ISMS via Dokobit Incident Management Procedure. More specifically:

A.16.1	Management of information security incidents and improvements	
A.16.1.1	Responsibilities and procedures	Incident Management Procedure represents a comprehensive workflow for managing information security incidents. The procedure is aligned with the GDPR and eIDAS requirements set for Qualified Trust Service Providers, relevant to the context and pre-filled forms, and represents all necessary responsibilities across Dokobit for reporting and handling an incident. For example, the Management group is responsible for the preparation of activities to deal with probable incidents; to ensure that appropriate logging and monitoring are in place; lessons-learned from previous incidents are integrated into Dokobit operations.
A.16.1.2	Reporting information security events	As per Incident Management Procedure, information security events might be detected internally by Dokobit controls or reported by internal or external parties.
A.16.1.3	Reporting information security weaknesses	As per Incident Management Procedure, information security events might be detected internally by Dokobit controls or reported by internal or external parties. Weaknesses are understood as flaws, faults, bugs, vulnerabilities, or other errors in software or hardware implementation, code, design, or architecture that if left unaddressed could result in systems, networks, or hardware being vulnerable to attack.
A.16.1.4	Assessment of and decision on information security events	Initial analysis phase of Incident Management Procedure defines assessment criteria towards security event. If the event is not confirmed as a security incident, it is forwarded for identification of corrective actions according to Dokobit Procedure for Corrective Action.
A.16.1.5	Response to information security incidents	The initial analysis phase of Incident Management Procedure defines assessment criteria towards a security event. If an event is confirmed as a security incident, it triggers further response actions (documented) based on best international practices (primarily NIST Special Publication 800-61, ENISA GDPR and eIDAS guidelines). Section Containment, eradication, and recovery represents response in details.
A.16.1.6	Learning from information security incidents	Incident Management Procedure defines post-incident activities, where lessons-learned analysis is performed and might result in risk reassessment, controls review, ISMS documentation update, and some specific improvement actions.
A.16.1.7	Collection of evidence	Incident Management Procedure, section Containment, eradication, and recovery represents requirements for evidence collection in the event of an incident or after it.

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 the legitimate request. Such information is managed in line with Dokobit Personal Data Protection Policy which is a part of Dokobit certified ISMS.

3.11 Business continuity management

Dokobit has implemented a business continuity management framework, which is a part of certified Dokobit ISMS and covers procedures of risk assessment, responses to incidents, disasters and their recovery plans including exercises.

The plans include all resources and processes necessary for the recovery and covers all the information security aspects of business continuity management. The objective of such plans is to complete the recovery of services within the set recovery time objective (RTO). Recovery plans are tested annually. More specifically:

A.17.1	Information security continuity	
A.17.1.1	Planning information security continuity	Disaster Recovery / Business Continuity Plan. The purpose of it 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). The Plan precisely addresses roles and responsibilities and triggers specific for every service plan, whose, when activated, restores services in an alternative pre-selected location in an automated manner.
A.17.1.2	Implementing information security continuity	Disaster Recovery / Business Continuity Plan addresses all relevant aspects of information security continuity and incorporates them in associated procedures. Dedicated section Information Security Continuity Aspects clarifies those aspects.
A.17.1.3	Verify, review and evaluate information security continuity	Due to nature of Dokobit activities, exposure to cloud services, Dokobit information security is resilient to disruptive events and, as per risk assessment and events in the past, no specific changes in ISMS are needed to be effective (actual and working) in the event of adverse situation.
A.17.2	Redundancies	

A.17.1	Information security continuity	
A.17.2.1	Availability of information processing facilities	Risk related to services availability are identified during risk assessment activities. Necessary actions are planned and implemented, including within the Disaster Recovery / Business Continuity Plan. Declared SLAs are monitored on a continuous basis. Information processing facilities are redundant in terms to comply with declared to clients RTOs.

3.12 TSP Termination and termination plans

Dokobit has up-to-date termination plan in accordance with clause 7.12 of ETSI EN 319 401.

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 Signature Validation Service by informing Customers and Supervisory body with a minimum notice of 3 months.

Reference: Dokobit Trust Services Termination Plan

3.13 Compliance

This section is covered by certified Dokobit ISMS via the Dokobit Procedure for Identification of Requirements. The procedure defines the process of identification of interested parties, as well as legal, regulatory, contractual and other requirements and responsibilities for their fulfilment. More specifically:

A.18.1	Compliance with legal and contractual requirements	
A.18.1.1	Identification of applicable legislation and contractual requirements	Procedure for identification of requirements defines the process of identification of interested parties, as well as legal, regulatory, contractual and other requirements related to information security, and responsibilities for their fulfilment. Activities result in the maintained and actual List of legal, regulatory, contractual and other requirements.
A.18.1.2	Intellectual property rights	Intellectual property rights are part of Business secrets defined by the board of management. It is regulated according to the EU and local legislation. Protection of intellectual property rights results in NDAs, contractual obligations and responsibilities and terms of Dokobit services.

A.18.1	Compliance with legal and contractual requirements	
A.18.1.3	Protection of records	Procedure for document and record control ensures control over creation, approval, distribution, usage and updates of documents and records used in the ISMS. In general, employees of the organization may access stored records by following principle “need to know” only.
A.18.1.4	Privacy and protection of personally identifiable information	Dokobit activities are subject to EU GDPR regulation, requirements of which are properly incorporated into the organisation, including ISMS documentation. From specific service/processes/asset owners perspective, service/processes/asset owners are responsible for each individual requirement identification (including contractual) and compliance within the asset. More information could be found in Procedure for Identification of Requirements.
A.18.1.5	Regulation of cryptographic controls	Policy on the Use of Cryptographic Controls defines rules (regulation) for the use of cryptographic controls, as well as the rules for the use of cryptographic keys, in order to protect the confidentiality, integrity, authenticity and non-repudiation of information. Policy on the Use of Cryptographic Controls also defines keys management, including their distribution practices.

4 Signature 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 unauthorized 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.

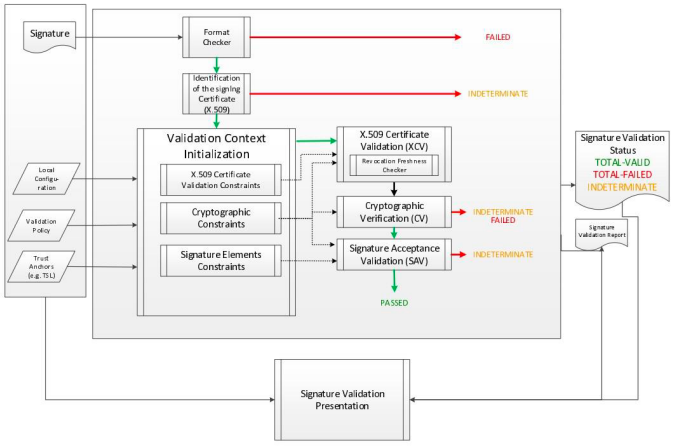
4.1 Signature validation process requirements

Dokobit validation service procedures for establishing whether an electronic signature or electronic seal is technically valid relay on the process described in ETSI TS 119 102 [ETSI119-102].

The following sections explain the way Dokobit validation service performs individual components of validation procedures, indicated the processes occurring and constraints. When no specific requirement is set in the present document, requirements and rules from ETSI TS 119 102 clauses 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 TS 119 102. In case of discrepancies between the present specifications and specifications from ETSI TS 119 102, the present specifications shall prevail.

4.1.1 Signature validation model



According to the conceptual model of Signature Validation defined in the referred specification, Dokobit Validation Service acts as a 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.

Driving Application (DA) for 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 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 – human-readable HTML page with an ability to download 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 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 TS 119 102-1, 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 into 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 specific signed attribute if present and considered validation evidences.
TOTAL-FAILED	The signature validation process results into 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 the signature to be TOTAL-PASSED or TOTAL-FAILED	The validation process outputs additional information to explain the INDETERMINATE indication and to help the verifier to identify what data is missing to complete the validation process.

In addition to the main status, the signature validation report also includes 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 why 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.
	HASH_FAILURE	The validation process shall provide: An identifier (s) (e.g. an 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 into 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 into 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 into TOTAL-FAILED because: • the signing certificate has been revoked; and • there is proof that the signature has been created after the revocation time.

Main indication	Sub-indication	Associated Validation report data	Semantics
	EXPIRED	The process shall output: The validated certificate chain	The signature validation process results into TOTAL-FAILED because there is proof that the signature has been created after the expiration date (notAfter) of the signing certificate
	NOT_YET_VALID	•	The signature validation process results into 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 into 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 into 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 into 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 were considered secure.	The signature validation process results into 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 into INDETERMINATE because a given formal policy file could not be processed for any reason (e.g. not accessible, not parse-able, digest mismatch, etc.).
	SIGNATURE_POLICY_NOT_AVAILABLE	•	The signature validation process results into 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 no respect the ordering constraints.	The signature validation process results into 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 into 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 into 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 into 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 into 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 into 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 into 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 were consider secure.	The signature validation process results into 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 into INDETERMINATE because a proof of existence is missing to ascertain that a signed object has been produced before some compromising event (e.g. 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 into 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 of time.
	SIGNED_DATA_NOT_FOUND	The process should output when available: The identifier(s) (e.g. an URI) of the signed data that caused the failure.	The signature validation process results into 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 contsraints 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 contsraints are defined in Annex B.*	1. 3.6.1.4.1.54720.1.3

- The signature validation service does not accept several sources of validation policy;
- The signature validation policy may not be ignored and replaced by signature validation roles 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 signature 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, signature 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, Dokobit validation service proceed 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.

The following electronic signature and electronic seal formats apply in the context of the EU legislation [EU 2015/1506] and are supported by 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

Validation process in Dokobit portal comprises of 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 one of QES validation policy or AdES validation policy;
3. Dokobit validation service validates document according to ETSI TS 119 102-1 and using selected validation policy.
4. The report is presented to the Subscriber.

Validation process in Dokobit Validation Service comprises of the following steps:

1. The Subscriber authenticates to the Service using electronic identification means;
2. The Subsriber uploads or selects electronically signed document and selects a validation policy. Dokobit validation service restricts validation policy to be one of QES validation policy or AdES validation policy;
3. Dokobit validation service validates document according to ETSI TS 119 102-1 and using selected validation policy.
4. The report is presented to the Subscriber.

Validation process in Dokobit Gateway and Dokobit validation service API comprises of 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 one of QES validation policy or AdES validation policy;
2. Dokobit validation service validates document according to ETSI TS 119 102-1 and using selected validation policy.
3. The report is returned in JSON response which contains a list of signatures and 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 Dokobit validation service provider and 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 following X.509 validation constraints which indicate requirements for use in the certificate path validation process as specified in ETSI TS 119 172-1 [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

Constraint(s)	Constraint value at signature validation (SVA or DA)
(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 appearing in 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 semantic applies 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 private key which is stored in Qualified Signature Creation Device as defined in [eIDAS]; expressed as a boolean.

Cryptographic Constraints

Dokobit validation service supports following cryptographic constraints which indicate requirements on algorithms and parameters used when creating signatures or used when validating signed object as specified in ETSI TS 119 172-1 [ETSI 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). They will be typically be represented by a list of entries as in table A.3.	Based on ETSI TS 119 312 [ETSI 119 312]

Signature and Seal Elements Constraints

Dokobit validation service supports following signature elements constraints which indicate requirements on the DTBS as specified in ETSI TS 119 172-1 [ETSI 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 the 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 indicate 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 EN 119 442.

Dokobit signature validation services are available at these means:

- as a REST API integration (Dokobit Gateway or Dokobit Validation Service API);
- as a Web Application with 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 the client can access 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 authorize using authorization access token, which ensures that uploaded information is accessible only for 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 out outside the control of the SVSP. Other trust service providers include time-stamping authorities, CRL and OCSP providers, 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 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 Advanced Electronic Seal with 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 support 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
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 (6 hours)	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 constraint is not met, validation shows error*
- *WARN - if constraint is not met, validation shows 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 support 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
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 (6 hours)	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 constraint is not met, validation shows error*
- *WARN - if constraint is not met, validation shows warning*
- *IGNORE - constraint is ignored*