AGENCY FOR DIGITAL GOVERNMENT

Den Danske Stat

VA Practice Statement

Contents

Changelog 4
References 4
1 Introduction 6
2 Definitions and abbreviations 8
3 General concepts 9
3.1 Validation services 9
3.2 Subscriber 9
3.3 Validation policy and VA Practice Statement 9
4 Validation Policies 10
4.1 Overview 10
4.2 Identification 10
4.3 User Community and Applicability 10
5 Introduction to validation policy and general requirements 11
5.1 General requirements 11
5.1.1 Publication 11
6 Policy and implementation 12
6.1 Risk assessment 12
6.2 VA practice statement 12
6.3 Terms and conditions 14
6.4 Information security policy 15
7 VA management and operation 17
7.1 Introduction 17
7.2 Internal organization 17
7.3 Personnel controls 18
7.4 Asset management 20
7.4.1 General requirements 20
7.4.2 Media handling 20
7.5 Access control 20
7.6 Cryptographic controls 21
7.6.1 General controls 21
7.7 Validation 21
7.7.1 General information about validation 21
7.7.2 Selecting validation processes 23
7.7.3 Status indication of the signature validation process and signature validation report 23
7.7.4 Validation constraints 24
7.7.5 Format checking 24

7.7.6 Identification of the signing or seal certificate 24
7.7.7 Validation context initialization 24
7.7.8 Revocation freshness checker 24
7.7.9 X.509 certificate validation 25
7.7.10 Cryptographic verification 25
7.7.11 Signature or seal acceptance validation 25
7.7.12 Validation presentation 25
7.7.13 Validation process for B-signatures 25
7.7.14 Time-stamp validation 25
7.7.15 Validation process for signatures with time stamps and signatures with long-term validation material 26
7.7.16 Validation process for signatures providing long-term availability 26
7.8 Physical and environmental security 26
7.9 Operation security 26
7.10 Network security 27
7.11 Incident management 29
7.12 Collection of evidence 31
7.13 Business Continuity Plan 32
7.14 VA termination and termination plans 32
7.15 Compliance 33

Changelog

Date	Version	Change description
30-9-2021	1.0	Initial version
5-11-2021	1.0.1	Changed usage of validation standard from ETSI TS 119 102-1 to ETSI EN 319 102-1. Updated description of supported algorithms.
06-02-2024	1.1	Updated based on new CP's

References

Term	Reference
[ASiC]	EN 319 162-1: Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers, v1.1.1, April 2016, ETSI ESI. https://www.etsi.org/standards
[CAdES]	ETSI EN 319 122-1: CAdES digital signatures Part 1: Building blocks and CAdES baseline signature, v1.3.1, June 2023, ETSI ESI. https://www.etsi.org/standards
[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
[ETSI EN 319 102-1]	ETSI EN 319 102-1, Electronic Signatures and Infrastructures (ESI) Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, v1.3.13, November 2021, ETSI ESI. An update to the standard is being prepared. https://www.etsi.org/standards
[ETSI TS 119 102-2]	ETSI TS 119 102-2: Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report, v1.4.1, June 2021, ETSI ESI. https://www.etsi.org/standards
[PAdES]	ETSI EN 319 142-1: AdES digital signatures; Part 1: Building blocks and PAdES baseline signatures, v1.2.1, April 2024, ETSI ESI. https://www.etsi.org/standards
[VA Policy]	Public policy for qualified signature and seal validation, Version 1.0, The Danish Agency for Digitisation, August 2020.

	https://certifikat.gov.dk/politikker-for-tillidstjenester/
[XAdES]	ETSI EN 319 132-1: XAdES digital signatures; Part 1: Building blocks and XAdES baseline signature, v1.2.1, February 2022, ETSI ESI. https://www.etsi.org/standards

1 Introduction

Den Danske Stat's Validation Service (VS) verifies electronic signatures and electronic seals (from this point forward denoted signature). The VS is provided to meet the requirements in [VA Policy] which again references the validation algorithm specified in [ETSI EN 319 102-1].

[ETSI EN 319 102-1] has passed ETSI ESI expert review and is currently on approval as an update to the existing European Norm. The VS uses this version as it contains an important correction to ensure that the VS correctly validates expired certificates used to produce revocation information when at the same time a valid time stamp token exist.

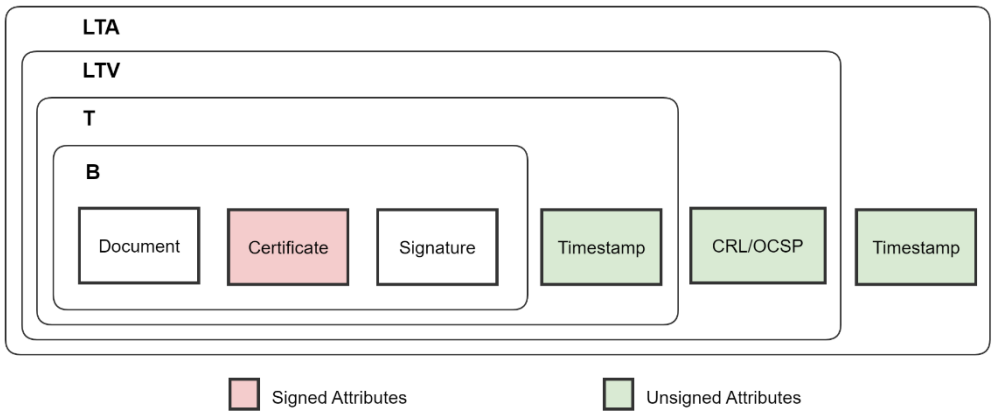
The VS verifies signatures to be compliant to the recognised standards [PAdES, XAdES, CAdES and ASiC] for advanced signature objects. Note that since the NemID produces a signature format different from the referenced standard formats, signatures generated by NemID cannot be verified by the VS.

The advanced signature formats are categorised in four groups each adding on top of the others, specific data to the signature to create a signature format, which meets a posed requirement.

In increasing order of complexity and data, the four groups are:

Group	Data	Security properties
Basic (B)	• Original document • Signed attributes (incl. signing certificate) • Signature	The signature can be used to prove that the identity in the signing certificate has produced a signature over the original document.
Time Stamp (T)	• Basic (B) • Time Stamp Token	The addition of the Time Stamp Token can be used to prove that the signature existed at the time specified in the token.
Long Term Validation (LTV)	• Time Stamp (T) • Revocation Information	The inclusion of Revocation Information proves that the signing certificate was not revoked at the time indicated in the information.
Long Term Archival (LTA)	• Long Term Validation (LTV) • Time Stamp Token	The Time Stamp Token proves that the Revocation Information was available at the time specified in the token.

The illustration below, describes how the classes are related.



The validation algorithm meets the requirement in [ETSI EN 319 102-1] and always instructs the validation algorithm to initiate the validation assuming the signature class to be LTA.

The VS uses a validation algorithm that implements the chain model. This provides signature validation results with a positive verdict even if the issuer of the subject certificate was revoked at the time of signing.

The VS uses the European List of Trusted List as source for accepted advanced and qualified certification authorities which are used as trust anchor for the validation algorithm. Besides the obvious, that the VS, can validate any signature created by a certificate which can be chained to the trust anchor and as an immediate result also certificates issued for local storage as part of NemID – of course subject to the certificate is used to produce a signature object compliant to profiles mentioned in the referenced standards.

The VS produces a signed validation report complaint to [ETSI TS 119 102-2].

This document describes the practices used by Den Danske Stat as Qualified Trust Service Provider to implement a Validation Authority that adheres to the danish policy [VA Policy] for qualified validation services.

Den Danske Stat Validation Authority is part of a Public Key Infrastructure, which also provides a Certification Authority with a remote Signing Service as well as Time Stamping.

Most of the requirements from [VA Policy] are similar to the general practices used by Den Danske Stat for implementing other qualified trust services. These are described in Den Danske Stat Certification Practice Statement [CPS] and whenever relevant referenced to from this document.

[REQ 1.3.4-01] Qualified trust service providers validating electronic signatures and electronic seals under this policy shall publish the policy on their website together with the EU trust label for qualified trust services on a 24/7 basis and without access control.

The validation policy is accessible via https://ca1.gov.dk. The EU Trust mark will be presented on the same site when the TSP is approved by supervisory body.

2 Definitions and abbreviations

Term	Description
PKI System	See [CPS]
Validation Authority (VA)	A VA is a Trusted Third Party that provides a Signature Validation Service.
Validation Service (VS)	A VS is a specific trusted service that offers signature validation.

3 General concepts

3.1 Validation services

The Validation Services (VS) consists of an infrastructure which provides validation services. This is provided by the Den Danske Stat's Validation Authority to the Subscribers and is part of the PKI offered by Den Danske Stat as a qualified trust service provider under the eIDAS regulation [eIDAS].

3.2 Subscriber

The Subscriber uses the VS through one of two means.

1. A natural person uses a web interface to the VS and uploads signed documents to be validated. The VS responds with a validation result, aimed to be easily understood by the person. In addition, the person has the option to download a signed validation report compliant with [ETSI TS 119 102-2]
2. System integration to the VS allows for any system to upload signed document for validation. In response, the system receives the same information as the natural person.

The Subscriber can be a natural person, legal person or a natural person associated to a legal person. In all cases, the Subscriber is can see its obligations on the Den Danske Stat's web site https://ca1.gov.dk.

3.3 Validation policy and VA Practice Statement

Den Danske Stat VA Practice Statement, this document, describes how the qualified trust service provider, Den Danske Stat, has met the requirements in the Danish policy for a qualified trust service providing VS.

4 Validation Policies

4.1 Overview

The Agency for Digitisation has established a trust service provider Den Danske Stat, which provides validation services which meets the requirements described in the eIDAS regulation [eIDAS].

The purpose is to provide end users in Denmark with an infrastructure that can provide validation services for electronic signatures and electronic seal used within public and private organisations.

The trust service provider Den Danske Stat acts as the legal entity providing validation services and bears the responsibility and liability for the services.

4.2 Identification

This version of the VA practice can be identified through the OID 1.2.208.169.1.2.3.1.0 - iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) practice-statements(2) validation(3) major-ver(1) minor-ver(1).

4.3 User Community and Applicability

The [VA Policy] does not pose any limitations on who are eligible to use the VS.

5 Introduction to validation policy and general requirements

5.1 General requirements

[REQ 5.1-01] VAs that validate electronic signatures or electronic seals under this policy shall be qualified trust service providers, see [eIDAS].

The validation service will be available as a qualified trust service when approved by the supervisory body

[REQ 5.1-02] The VA shall comply with requirements specified in articles 32, 33 and 40 of eIDAS.

The VS validates certificates with the EU LOTL as trust anchor. The qualified or non-qualified status of the certificate is determined from the LOTL.

The validation process relies on timestamps in order to determine a point of existence for which the signature is known to exists.

The complete signed data object including the data that has been signed is submitted to the VS for validation.

The validation result covers that the subject name attributes are made available for the relying party. The name attribute may cover that a pseudonym was used in the certificate and in this case, this is returned with a clear indication that it is a pseudonym.

The certificate qcStatement extension (0.4.0.1862.1.4) is used to check if a qualified signature creation device was used to manage the signature private key.

During the signature validation, the signature value is verified to be intact.

The VS supports signature formats as specified in [ASiC, CAdES, PAdES and XAdES].

The validation report provides a result of the validation including details on any security related issues identified during signature validation.

The VS is offered by the qualified trust service provider Den Danske Stat VA.

5.1.1 Publication

Den Danske Stat's Practice Statement for the Validation Authority is published at https://ca1.gov.dk/practice

6 Policy and implementation

6.1 Risk assessment

[REQ 6.1-01] The VA shall carry out a risk assessment to identify, analyse and evaluate business and technical risks.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5-02 for details.

[REQ 6.1-02] The VA shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5-03 for details.

[REQ 6.1-03] The VA shall determine and document all security requirements and operational procedures that are necessary to comply with this policy. The documentation must be part of the VA practice statement, cf. clause 6.2.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5-04 for details.

[REQ 6.1-04] The risk assessment shall be reviewed and revised at least once a year.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5-05 for details.

[REQ 6.1-05] The VA's management shall approve the risk assessment and accept the residual risk identified.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5-06 for details.

6.2 VA practice statement

[REQ 6.2-01] The VA shall specify a VA practice statement addressing all requirements of this policy. This VA practice statement shall include all external organizations supporting the VA's services and shall conform to this policy. The VA practice statement may be divided into a public and private part, with the public part of the VA practice statement being published.

This document constitutes the VA practice statement.

For further details this requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 1.5.4-01 and REQ 2.1-03 for details.

[REQ 6.2-01A] When the VA makes use of other parties, including trust service component providers through subcontracting, outsourcing or other third party arrangements, the CA shall maintain the overall responsibility for meeting the requirements of this policy.

See CPS REQ 1.5.4-01A

[REQ 6.2-01B] When the VA makes use of a trust service component provided by another party, the VA shall ensure that the use of the component interface meets the requirements as specified by the provider.

See CPS REQ 1.5.4-01B

[REQ 6.2-01C] When the VA makes use of a trust service component provided by another party, the VA shall ensure the necessary security and functionality required for compliance with this policy.

See CPS REQ 1.5.4-01C

[REQ 6.2-02] The management of the VA shall be responsible for and approve the entire VA practice statement and ensure correct implementation, including that the practice statement complies with this policy and is communicated to relevant employees and partners.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 1.5.4-07 for details.

[REQ 6.2-03] The VA shall make the public part of the VA's applicable practice statement available on the VA's website on a 24/7 basis.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 2.1-02 for details.

[REQ 6.2-04] The VA practice statement shall be reviewed and revised on a regular basis and at least once a year. The responsibility for maintaining the VA practice statement must be determined and documented. Changes in the VA practice statement must be documented.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 1.5.4-08 and REQ 2.1-06 for details.

[REQ 6.2-05] In the VA practice statement, the VA shall specify provisions upon termination of the service. These must at a minimum include information on who will be notified upon termination and who will take over customers and users, if these types of agreements exist.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-02 for details.

[REQ 6.2-06] The public part of the VA practice statement must as a minimum include:

- **a) an indication of the CA root certificates included in the VA's trust anchor;**
- **b) any limitations on the use of the validation service;**
- **c) the subscriber's obligations, if any**

Ad a) In this context, a Trusted Services List (TSL) is a list of trusted services covering their qualification and their certificate. It is provided by an authoritative source, typically an EU member state. The Danish Trusted List is provided by the Agency for Digitisation and located their website.

The TSL is signed by the issuer and any usage of the list requires the signature to be validated, e.g. by using the signing certificate as part of the TSL.

The EU List of Trusted List (LOTL) is a collection of TSLs. The collection is signed by signed by the EU commission using a key pair published by the EC: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52019XC0816(01)&from=EN

The key pairs provided on this list is used as the single point of trust by the validation engine. The LOTL and the national TSLs are periodically retrieved and the signature of the entities verified. Initially the signature of the LOTL is verified, and after that the signature of each TSL is verified. The collection of service certificates

for certification authorities on the TSLs is used as trust anchor by the Validation Service. Any certificate to be validated, must have a valid certificate path containing one of the service certificates on the chain.

Ad b) No limitations except for fair use is applied to the service. The service may be limited at a later stage without prior notice.

Ad c) The service includes [Terms] of using the service which includes obligations for the relying party.

[REQ 6.2-07] The VA practice statement should contain any uptime limitations in the VA's service.

This VS is available 24/7. Any maintenance windows or planned disruption of the service is communicated at https://ca1.gov.dk.

6.3 Terms and conditions

[REQ 6.3-01] The VA shall make the terms and conditions regarding its services available to all subscribers and relying parties.

Term and conditions are published at https://ca1.gov.dk/

[REQ 6.3-02] The terms and conditions shall include:

- **a) a description of the service, including what policies are covered by the service;**
- **b) any limitations on the use of the service;**
- **c) the subscriber's obligations, if any;**
- **d) information for parties relying on the trust service;**
- **e) the period of time during which event logs are retained;**
- **f) limitations of liability;**
- **g) limitations on the use of service, including the VA's limitation of liability in terms of wrong use of the service;**
- **h) the applicable legal system;**
- **i) dispute procedures;**
- **j) that the VA is a qualified trust service, cf. the eIDAS Regulation;**
- **k) The VA's contact information, and**
- **l) any undertaking regarding availability.**

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 2.1-03 for details.

[REQ 6.3-03] Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

Term and conditions are published at https://ca1.gov.dk/

[REQ 6.3-04] Terms and conditions shall be made available through a durable means of communication.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 2.1-06 for details.

[REQ 6.3-05] Terms and conditions shall be available in a readily understandable language.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 2.1-07 for details.

[REQ 6.3-06] Terms and conditions may be transmitted electronically.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 2.1-08 for details.

[REQ 6.3-07] The VA shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters and such policies and procedures shall comply with the VA's terms and conditions.

Den Danske Stat VA has procedures for the resolution of complaints and disputes received from customers or other relying parties.

[REQ 6.3-08] If a dispute cannot be resolved out of court, either party may choose to bring the dispute before the ordinary courts of law. The venue is the City of Copenhagen. Subject to Danish law.

Terms & conditions includes dispute management procedures which ultimately either party may choose to bring the dispute before the ordinary courts of law. The venue is the City of Copenhagen. Subject to Danish law.

6.4 Information security policy

[REQ 6.4-01] The VA shall comply to the requirements in the information security standard ISO 27001 and shall be able to document compliance through e.g. certification.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.2-01 for details.

[REQ 6.4-02] The VA shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.2-02 for details.

[REQ 6.4-03] Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, conformity assessment body, supervisory body or other authorities.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.2-03 for details.

[REQ 6.4-04] The VA's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for the VA's facilities, systems and information assets providing the services.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.2-04 for details.

[REQ 6.4-05] The VA shall publish and communicate the information security policy to all employees who are impacted by it, including employees at outsourcers performing work for the VA.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.2-05 for details.

[REQ 6.4-06] The VA shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the VA's functionality is undertaken by outsourcers.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9.6.1-01 for details.

[REQ 6.4-07] The VA shall set out and ensure efficient implementation of relevant controls at the outsourcers.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9.6.1-01 for details.

[REQ 6.4-08] The VA's information security policy and inventory of assets for information security shall be reviewed at annually and if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.2-06 for details.

[REQ 6.4-09] Any changes that may impact on the level of security provided shall be approved by the VA's management.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.2-07 for details.

[REQ 6.4-10] The configuration of the VA's systems shall be checked at fixed intervals and at least once a year for changes which violate the VA's information security policy.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.2-08 for details.

[REQ 6.4-11] The maximum interval between two of the above checks shall be documented in the VA practice statement.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.2-10 for details.

7 VA management and operation

7.1 Introduction

[REQ 7.1-01] The VA shall have a system or systems for quality and information security management appropriate for the validation services provided.

Den Danske Stats TSA implements ISO/IEC 27001.

7.2 Internal organization

[REQ 7.2-01] The VA shall be a legal entity.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 1.3.1-02 for details.

[REQ 7.2-02] The VA organization shall be reliable and non-discriminatory.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9-01 for details.

[REQ 7.2-03] The VA should make its services accessible to all applicants whose activities fall within its declared field of operation and make sure that they abide by their obligations as specified in the VA's terms and conditions.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9-02 for details.

[REQ 7.2-04] The VA shall maintain sufficient financial resources and/or obtain appropriate liability insurance in accordance with applicable law, including eIDAS, to cover liabilities arising from its operations and/or activities.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9.2.1-01.

[REQ 7.2-05] If the VA is a private enterprise, the VA shall obtain and maintain liability insurance, cf. REQ 7.2-04. Such insurance shall as a minimum provide a coverage of DKK 25 million per year.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 7.7.2-07 and REQ 9.2.1-02 for details.

[REQ 7.2-06] The VA shall have the financial stability and resources required to operate in conformity with this policy.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9.2.2.-01 for details.

[REQ 7.2-07] The VA shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9.13-01 for details.

[REQ 7.2-08] The VA shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third-party arrangements.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9.17-01 for details.

[REQ 7.2-09] Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the VA's assets.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.1-05 for details.

7.3 Personnel controls

[REQ 7.3-01] The VA shall ensure that employees and contractors support the trustworthiness of the VA's operations.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.3-01 for details.

[REQ 7.3-02] The VA shall employ a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type and volume of work necessary to provide validation services.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS 5.3.1-01 for details.

[REQ 7.3-03] The VA's personnel, including personnel of any subcontractors, should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.3.3-01 for details.

[REQ 7.3-04] The VA shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding information security and personal data protection rules as appropriate for the offered services and the job function.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.3-01 for details.

[REQ 7.3-05] The above training requirements should encompass regular (at least every 12 months) updates concerning new threats and current security practices.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.3.4-01 for details.

[REQ 7.3-06] Appropriate disciplinary sanctions shall be applied to personnel violating the VA’s policies or procedures.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.3.6-02 for details.

[REQ 7.3-07] Security roles and responsibilities as specified in the VA’s information security policy shall be documented in job descriptions or in documents available to all concerned personnel.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.3.1-03 for details.

[REQ 7.3-08] Trusted roles, on which the security of the VAs operation is dependent, shall be clearly identified and approved by the management.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.1-01 for details.

[REQ 7.3-09] Trusted roles shall be approved by the management and accepted by the person to fulfil the role.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.3-02 for details.

[REQ 7.3-10] The VA's personnel (both temporary and permanent) shall have job descriptions defined from the viewpoint of roles fulfilled with segregation of duties and least privilege, the sensitivity of data that can be accessed, background screening and employee training and awareness.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.3-03 for details.

[REQ 7.3-11] Where appropriate, job descriptions shall differentiate between general functions and the VA's specific functions. These should include skills and experience requirements.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.3-04 for details.

[REQ 7.3-12] Personnel shall exercise administrative and management procedures and processes that are in line with the VA's information security management procedures.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.3.6-01 for details.

[REQ 7.3-13] Managerial personnel shall possess experience or training with respect to operation of the VA, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions for the VA.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.3.1-02 for details.

[REQ 7.3-14] All the VA's personnel in trusted roles shall be free from conflicts of interest that might prejudice the impartiality of the VA's operations.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.1-03 for details.

[REQ 7.3-15] Trusted roles shall include roles that involve the following responsibilities:

a) **Security Officers: Overall responsibility for administering the implementation of the security practices.**
b) **System Administrators: Authorized to install, configure and maintain the VA's critical systems for service management, including system restoration.**
c) **System Operators: Responsible for operating the VA's critical systems on a day-to-day basis. Authorized to perform system backups.**
d) **System Auditors: Authorized to view archives and audit logs of the VA's critical systems.**

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.1-04 for details.

[REQ 7.3-16] Personnel that are to access or configure privileges for trusted roles shall be formally approved by a security manager at the senior management level. This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.3-01 for details.

[REQ 7.3-17] Personnel shall not have access to the trusted functions until the necessary checks are completed.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.3-05 for details.

7.4 Asset management

7.4.1 General requirements

[REQ 7.4.1-01] The VA shall maintain an inventory of its assets, including information assets. All information assets shall be classified according to the VA's risk assessment, and the VA shall ensure adequate protection of all assets.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5-07 for details.

7.4.2 Media handling

[REQ 7.4.2-01] All media in the VA's operating system shall be handled securely in accordance with its classification, and

- **media containing sensitive data shall be securely disposed of when no longer required;**
- **media shall be protected from damage, theft, unauthorized access and obsolescence; and**
- **sensitive data shall be protected against unauthorized access through re-used storage objects.**

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.1.6-01 and REQ 5.1.7-01 for details.

7.5 Access control

[REQ 7.5-01] The VA shall implement effective access control that protects against unauthorized physical or logical access to the VA's systems. In particular: see REQ 7.5-02 to 7.5-09

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5-08 for details.

[REQ 7.5-02] The VA shall implement controls (e.g. firewalls) to protect the VA's internal network from unauthorized access, including access by subscribers and relying parties.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-01 for details.

[REQ 7.5-03] Firewalls shall also be configured to prevent all protocols and accesses not required for the operation of the VA.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-13 for details.

[REQ 7.5-04] The VA shall implement an efficient user administration, including administer user access of operators, administrators and system auditors applying the principle of "least privileges".

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.3-01 for details.

[REQ 7.5-05] User accounts shall be checked regularly to ensure that the users at all times only have the necessary rights, cf. access control policy.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.3-02 for details.

[REQ 7.5-06] Access to information and application system functions shall be restricted in accordance with the access control policy.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.3-03 for details.

[REQ 7.5-07] The VA's operating systems shall provide sufficient computer security controls for the separation of trusted roles identified in the VA's practice statement, including the separation of security administration and operational roles. Particularly, use of system utility programs shall be restricted and controlled to what is necessary.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.5.1-01 for details.

[REQ 7.5-08] The VA's personnel shall be identified and authenticated before using critical systems and applications.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.3-04 for details.

[REQ 7.5-09] The VA's personnel shall be accountable for their activities., e.g. through efficient event logging.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.3-05 for details.

7.6 Cryptographic controls

7.6.1 General controls

[REQ 7.6.1-01] The VA shall implement secure handling of cryptographic keys and cryptographic devices. The handling shall cover the full lifecycle of keys and devices.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.1.1-02 for details.

7.7 Validation

7.7.1 General information about validation

[REQ 7.7.1-01] The service provided by the VA for validation of electronic signatures and electronic seals under this policy shall validate electronic signatures and electronic seals in accordance with the policy, while considering any constraints as described below or in the public part of the VA's practice statement.

The validation constraints are divided into three subsections:

- X.509 Validation Constraints
- Cryptographic Constraints
- Signature Elements Constraints

X.509 Validation Constraints

- Model is set to use the chain model.
- SetOfTrustAnchors is set to use the EU LOTL
- CertificationPath and path-length-constraints are not configured. There are no constraints on the length of the certificates path, except any constraints described in certificates in the certificate path (i.e. basicConstraints).
- On polices: user-initial-policy-set, initial-policy-mapping-inhibit, initial-explicit-policy, initial-any-policy-inhibit and policy-constraints are not configured as the Validation Service is aimed to be used to validate certificates which have a trust anchor in the LOTL. This scheme does not support cross certification and the mapping is not used.
- initial-permitted-subtrees and initial-excluded-subtrees are used as there are no naming re-strictions in the Validation Service.
- RevocationCheckingConstraints is configures to require revocation data to be available.
- RevocationFreshnessConstraints is not configured to a specific value. Freshness is determined by inspection of OCSP and CRL dates as specified in [ETSI EN 319 102-1], clause 5.2.5.
- RevocationInfoOnExpiredCerts is not configured as there is no time limit for TSPs to provide revocation information on expired certificates.
- LoAOnTSPPractices is implicitly configured as the Validation Service accepts all certificates issued by certification authorities in the trust anchor.

Cryptographic Constraints

- Cryptographic suites
    - The following digest algorithms are supported: SHA256, SHA384 and SHA512
    - The following signature key sizes are supported: RSA2048, RSA4096, ECDSA256, ECDSA384 and ECDSA512 using Brainpool and NIST recommended elliptic curves.

Signature Elements Constraints

- ConstraintOnDTBS is not configured as the Validation Service does not require specific types of data being signed beside those imposed by the signature format.
- ContentRelatedConstraintsAsPartOfSignatureElements is not configured as the Validation Service does not pose any constraints of the content which the signature covers.
- DOTBSAsAWholeOrInParts is not configured as the Validation Service does not impose any constraints on whether the data to be signed is provided as a whole or in parts. Any requirements on this are managed by the supported signature formats.

[REQ 7.7.1-02] The VA shall present the validation result, including relevant details and any constraints relevant to the validating party, who must interpret the result.

The information made available to the user covers:

- The terms and conditions for using the Validation Service.

- A signature validation status with value TOTAL PASSED, TOTAL FAILED or INDETERMINATE. The status is highlighted in green, red or yellow to emphasize the result.
- The Validation Service only covers one signature validation policy described in [VA Policy], namely: Denne politik er identificeret som ”Offentlig politik for kvalificeret signatur- og seglvalidering - Version 1.0”
- The validation time indicating the time of the validation
- The best signature time indicating the time at which the validation algorithm could determine the signature was present. For an AdES level B this should be the validation time, for AdES level LTA this should be the time within the archive time stamp.
- The validation process which has been used for the validation.
- The complete validation data as specified in [ETSI TS 119 102-2].

[REQ 7.7.1-03] Unless the validating party requests otherwise, the validation shall start with ‘Validation process for Signature providing Long Term Availability and Integrity of Validation Material’, see clause 5.6.3 of [ETSI EN 319 102-1].

The validation service always attempts to validate signature following [ETSI EN 319 102-1, section 5.6.3].

[REQ 7.7.1-04] The status on a validation shall be one of the following:

TOTAL-PASSED: when the cryptographic checks of the signature (including checks of hashes of individual data objects that have been signed indirectly) succeeded as well as all checks described in this policy have been passed.

TOTAL-FAILED: when the cryptographic checks of the signature failed (including checks of hashes of individual data objects that have been signed indirectly), or it is proven that the generation of the signature or seal after the revocation of the signing certificate, or because the signature or seal is not conformant to one of the base standards to the extent that the cryptographic verification building block is unable to process it.

INDETERMINATE: when the results of the performed checks do not allow to ascertain the signature or the seal to be TOTAL-PASSED or TOTAL-FAILED

See REQ 7.7.1-02

[REQ 7.7.1-05] The above status shall be accompanied by detailed information as specified in clause 5.1.3 of [ETSI EN 319 102-1].

See REQ 7.7.1-02.

7.7.2 Selecting validation processes

[REQ 7.7.2-01] All requirements in clause 5.1.2 of [ETSI EN 319 102-1] shall be complied with.

The validation service always attempts to validate signature following [ETSI EN 319 102-1, section 5.6.3.

[REQ 7.3-17] Personnel shall not have access to the trusted functions until the necessary checks are completed.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.3-05 for details.

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

[REQ 7.7.3-01] All requirements in clause 5.1.3 of [ETSI EN 319 102-1] shall be complied with.

See REQ 7.7.1-02.

7.7.4 Validation constraints

[REQ 7.7.4-01] All requirements in cause 5.1.4 of [ETSI EN 319 102-1] shall be complied with.

See REQ 7.7.1-01.

7.7.5 Format checking

[REQ 7.7.5-01] The format shall be checked in conformity with clause 5.2.2 of [ETSI EN 319 102-1].

Section 5.2.2 of [ETSI EN 319 102-1] does not have any explicit requirements.

7.7.6 Identification of the signing or seal certificate

[REQ 7.7.6-01] The signing or seal certificate shall be identified in conformity with clause 5.2.3 of [ETSI EN 319 102-1].

Identification of the signing certificate is required in order to figure out which certificate shall be used to verify the signature. A signature object may contain several certificates, supplied by the signature creator with the intension to aid signature validation. A mean to easily identity the signing certificate is to provide a signed attribute referencing the signing certificate. This attribute is mandatory for the [PAdES, XAdES, CAdES and ASiC] formats supported by public services within EU.

The validation service is configured to require the signing certificate to be present within the signature object and referenced from a signed attribute identifying the certificate.

7.7.7 Validation context initialization

[REQ 7.7.7-01] Validation context shall be initialized in conformity with clause 5.2.4 of [ETSI EN 319 102-1].

The Validation context initialization uses all data elements mentioned in clause 5.2.4 of [ETSI EN 319 102-1]:

- the Signed data object,
- the default configured validation policy, and
- the trust anchor to a validation context.

7.7.8 Revocation freshness checker

[REQ 7.7.8-01] Checks that a given revocation status information is fresh shall be made in conformity with clause 5.2.5 of [ETSI EN 319 102-1].

Revocation freshness is used to determine if revocation status information is updated or fresh at the time when it is used for validation. The validation time is the time at which the validation occurs and is typically the current time. The time used for validation is likely closer to the time at which the signature was created.

There are two choices for how updated information is determined.

1) Either it is configured as time span around the thisUpdate in the revocation information data

or

2) It is calculated using the thisUpdate and nextUpdate

Now, as the VS uses revocation information from sources, which may have different life spans, i.e. the validity of revocation information provided by root CAs may be longer than revocation information provided by issuing CAs, option 1) is not feasible or would require a configuration for freshness being beyond

reasonable acceptable expectations for cases where the update period is very different for the CAs (as it is for e.g. Den Danske Stat Root CA and Den Danske Stat Issuing CA issuing CRL), option 2 is used.

7.7.9 X.509 certificate validation

[REQ 7.7.9-01] The signing or seal certificate shall be validated in conformity with clause 5.2.6 of [ETSI EN 319 102-1]. The chain model shall be supported and the shell model may be supported.

The purpose of X.509 certificate validation is to find a prospective certificate path from the signing certificate to a certificate in the trust anchor and validate its validity meeting the validation constraints at the time of the validation.

The X.509 certificate validation uses the signing certificate, trust anchor, configured constraints, revocation information and time to find a certificate path. Recall from REQ 7.7.1-01 that the chain model is always used.

[REQ 7.7.9-02] The VA shall specify the models being supported in the public part of the VA's practice statement.

See REQ 7.7.1-01.

7.7.10 Cryptographic verification

[REQ 7.7.10.-01] The cryptographic integrity of the signed data shall be in conformity with clause 5.2.7 of [ETSI EN 319 102-1].

The Cryptographic verification uses the signed document (including the signature), signing certificate and cryptographic constraints and performs and conducts cryptographic verification on the signature.

7.7.11 Signature or seal acceptance validation

[REQ 7.7.11.-01] Additional verification of signature or seal to be performed in conformity with clause 5.2.8 of [ETSI 319 102-1].

Signature acceptance validation (SAV) covers additional verification steps beside the Format Check. The Validation Service checks that the signature structure is correct, that the signing-time attribute is present (either directly or as part of the PDF in case it is PAdES), the digest of the signed data can be located and that the cryptographic constraints are met.

7.7.12 Validation presentation

[REQ 7.7.12.-01] Validation presentation shall be made in conformity with clause 5.2.9 of [ETSI EN 319 102-1].

See REQ 7.7.1-02.

7.7.13 Validation process for B-signatures

[REQ 7.7.13.-01] Validation of a B-signature shall be in conformity with clause 5.3 of [ETSI EN 319 102-1].

See REQ 7.7.13-01.

7.7.14 Time-stamp validation

[REQ 7.7.14.-01] Validation of time stamps shall be in conformity with clause 5.4 of [ETSI EN 319 102-1].

See REQ 7.7.13-01.

7.7.15 Validation process for signatures with time stamps and signatures with long-term validation material

[REQ 7.7.15.-01] Validation of signatures with time stamps and signatures with long-term validation material shall be in conformity with clause 5.5 of [ETSI EN 319 102-1].

See REQ 7.7.13-01.

7.7.16 Validation process for signatures providing long-term availability

[REQ 7.7.16.-01] Validation process for signatures providing long term availability shall be in conformity with clause 5.6 of [ETSI EN 319 102-1].

See REQ 7.7.13-01.

7.8 Physical and environmental security

[REQ 7.8-01] The VA shall control physical access to components of the VA's system based on the classification policy. This includes minimizing risks related to physical security.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.1-01 for details.

[REQ 7.8-02] The VA shall ensure that access to facilities is limited to authorized individuals.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.1.1-02 for details.

[REQ 7.8-03] The VA shall implement effective protection to avoid

- **loss, damage or compromise of assets and interruption to business activities; and**
- **compromise or theft of information and information processing facilities.**

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.1-02 for details.

[REQ 7.8-04] Components that are critical for the secure operation of the VA shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.1.2-02 for details.

[REQ 7.8-11] Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.1.2-07 for details.

7.9 Operation security

[REQ 7.9-01] The VA shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.1-01 for details.

[REQ 7.9-02] The VA shall ensure that, prior to any system development (e.g. undertaken by the VA or on behalf of the VA), a plan approved by management is provided to ensure that security is built into the systems. The plan shall include an analysis of security requirements being met in order to maintain an adequate level of security.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.1-02 for details.

[REQ 7.9-03] The VA shall implement documented processes for release and change management of software, hardware and configuration changes. The VA shall have documented processes for security update of proprietary and standard software and firmware. The processes shall include documentation of the changes.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.5.1-02 for details.

[REQ 7.9-04] The integrity of the VA's systems and information shall be protected against viruses, malicious and unauthorized software, and the VA shall implement processes for ensuring that:

- **security patches are applied within a reasonable time after they come available;**
- **security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and**
- **the reasons for not applying any security patches are documented.**

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.5.1-03 for details.

[REQ 7.9-05] Media used within the VA's systems shall be securely handled according to the classification and to protect media from damage, theft, unauthorized access and obsolescence.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.1.6-01 for details.

[REQ 7.9-06] The VA shall have media management procedures in place to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.1.6-02 for details.

[REQ 7.9-07] The VA shall establish and implement procedures for all trusted and administrative roles that may impact on the VA's security and operations.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.2.1-02 for details.

[REQ 7.9-08] The VA shall plan and monitor future capacity requirements made to ensure that adequate processing power and storage are available at all times.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.6.3-06 for details.

7.10 Network security

[REQ 7.10-01] The VA shall protect its network and systems from attack and unauthorized access.

In particular: see REQ 7.10-02 to 7.10-05, 7.10-07 and 7.10-09 to 7.10-16

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-01 for details.

[REQ 7.10-02] The VA shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationships between critical systems and services.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.1.1-03 for details.

[REQ 7.10-03] The VA shall apply the same security controls to all systems co-located in the same zone.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-07 for details.

[REQ 7.10-04] The VA shall restrict access and communications between zones to those necessary for the operation of the VA.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS 6.7-13 for details.

[REQ 7.10-05] The VA shall explicitly forbid or deactivate not needed connections and services.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-13 for details.

[REQ 7.10-07] The VA shall review the established network and firewall rules set on a regular basis.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-15 for details.

[REQ 7.10-09] The VA shall place particularly critical systems in high-security zones.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-08 for details.

[REQ 7.10-10] The VA shall separate dedicated networks for administration of IT systems and the VA's operational network.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-10 for details.

[REQ 7.10-11] The VA shall not use systems used for administration of the security policy implementation for other purposes.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-11 for details.

[REQ 7.10-12] The VA shall separate the production systems from systems used in development and testing.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-12 for details.

[REQ 7.10-13] The VA shall establish communication between critical systems only through trusted channels that are physically or logically distinct from other communication channels and provide confidentiality, integrity and authenticity between the systems.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-14 for details.

[REQ 7.10-14] If a high level of availability of external access to the trust service is required, the external network connection shall be redundant.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-16 for details.

[REQ 7.10-15] The VA shall undertake vulnerability scan from external and internal IP-addresses at least once every quarter. The vulnerability scans shall be performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report. Scans shall be documented.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-17 for details.

[REQ 7.10-16] The VA shall perform a penetration test at least once a year, after set up and in case of significant infrastructure or application upgrades or modifications. The penetration test shall be performed by a person or entity with the skills, tools, code of ethics and independence necessary to provide a reliable report. The penetration test shall be documented.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.7-18 for details.

7.11 Incident management

[REQ 7.11-01] System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored.

In particular: see REQ 7.11-02 to 7.11-12

See REQ 7.11-02 to 7.11.12 for details

[REQ 7.11-02] Monitoring activities must take account of the sensitivity of any information collected or analysed.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-02 for details.

[REQ 7.11-03] Abnormal system activities that indicate a potential security violation, including intrusion into the VA's network, shall be detected and reported as alarms.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-03 for details.

[REQ 7.11-04] The VA shall monitor the following events:

a) **start-up and shutdown of the logging functions; and**
b) **availability and utilization of needed services with the VA's network.**

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-04 for details.

[REQ 7.11-05] The VA shall act in a timely and co-ordinated manner in order to respond quickly to security events and to limit the impact of breaches of security.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-05 for details.

[REQ 7.11-06] The VA shall appoint trusted role personnel to follow up on alerts of potentially critical security events to ensure that relevant incidents are reported in line with the VA's procedures.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-06 for details.

[REQ 7.11-07] The VA shall have procedures and emergency preparedness that ensure notification of a security event or loss of integrity to relevant parties, cf. applicable regulations, for example the data protection authorities and/or the eIDAS supervisory body at the latest 24 hours after the event has been identified.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-07 for details.

[REQ 7.11-08] Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person, the VA shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-08 for details.

[REQ 7.11-09] The VA's systems must be monitored, which must encompass monitoring or regular review of audit logs in order to identify malicious activity for purposes of sending alarms for potential critical security events to security personnel.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-09 for details.

[REQ 7.11-10] The VA shall address any critical vulnerability not previously addressed by the VA within a period of 48 hours after its discovery.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-10 for details.

[REQ 7.11-11] For any vulnerability, given the potential impact, the VA shall either:

- **a) create and implement a plan to mitigate the vulnerability; or**
- **b) document the factual basis for the VA's determination that the vulnerability does not require remediation.**

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-11 for details.

[REQ 7.11-12] Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.1-12 for details.

7.12 Collection of evidence

[REQ 7.12-01] The VA shall record and keep accessible for an appropriate period of time, including after the activities of the VA have ceased, all relevant information concerning data issued and received by the VA in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. In particular: see REQ 7.12-02 to 7.12-08

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.5.1-01 for details.

[REQ 7.12-02] The VA shall maintain the confidentiality and integrity of archived records concerning operation of its services.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.5.3-01 for details.

[REQ 7.12-03] The VA shall ensure the completeness, confidentiality and integrity of archived records concerning the operation of its services in accordance with disclosed business practices.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.5.3-02 for details.

[REQ 7.12-04] Records, including audit log, shall be made available if required for the purposes of providing evidence in legal proceedings.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.5.7-01 for details.

[REQ 7.12-05] The precise time of significant environmental, key management and clock synchronization events shall be recorded.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.8-02 for details.

[REQ 7.12-06] The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 6.8-01 for details.

[REQ 7.12-07] Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the VA's terms and conditions.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.5.2-01 for details.

[REQ 7.12-08] The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-06 for details.

7.13 Business Continuity Plan

[REQ 7.13-01] The VA shall define, test and maintain a Business Continuity Plan (BCP) to enact in case of a disaster.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.4-01 for details.

[REQ 7.13-02] In the event of a disaster, including compromise of one of the VA's private signing keys, where such keys exist, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster with appropriate remediation measures.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.7.4-02 for details.

7.14 VA termination and termination plans

[REQ 7.14-01] Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the VA's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.

In particular: see REQ 7.14-02 to 7.14-09 and 7.14-11 to 7.14-12

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-05 for details.

[REQ 7.14-02] The VA shall have an up-to-date termination plan.

Before the VA terminates its services, the following procedures apply, see REQ 7.14-03 to 7.14-08

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-01 for details.

[REQ 7.14.03] a) Before the VA terminates its services, the VA shall inform the following of the termination: all subscribers and other entities with which the VA has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-03 for details.

[REQ 7.14-04] b) Before the VA terminates its services, the VA shall make the information of the termination available to other relying parties.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-03 for details.

[REQ 7.14-05] c) Before the VA terminates its services, the VA shall terminate authorization of all subcontractors to act on behalf of the VA in carrying out any functions relating to the process of validating electronic signatures and electronic seals.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-07 for details.

[REQ 7.14-06] d) Before the VA terminates its services, the VA shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the VA for a reasonable period, unless it can be demonstrated that the VA does not hold any such information.

Due to the nature of the Den Danske Stat VA currently no other TSP are identified which can take over the delivery of Den Danske Stat's services.

Den Danske Stat VA has a termination plan which ensures that the required information is available for a reasonable period.

[REQ 7.14-07] e) In connection with the VA terminating its services, the VA's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-08 for details.

[REQ 7.14-08] f) Where possible the VA should make arrangements to transfer provision of trust services for its existing customers and users to another VA.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-09 for details.

[REQ 7.14-09] When the VA terminates its services, the VA shall maintain its obligations to make available its public keys to relying parties for a reasonable period or transfer such obligations to another reliable party.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-05 for details.

[REQ 7.14-11] Where the VA is a private business, the VA shall provide an irrevocable demand guarantee or the like with an approved institute to secure payment of its financial obligations in accordance with REQ 7.14-1 to REQ 7.14-09.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-11 for details.

[REQ 7.14-12] The VA shall state in its practices the provisions made for termination of service. This shall include:

a) **information about the affected entities to be notified; and**
b) **who will take over customers and users, where such form of agreement is available.**

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5.8-02 for details.

7.15 Compliance

[REQ 7.15-01] The VA shall ensure that it operates in a legal and trustworthy manner as a qualified trust service that validates electronic signatures and electronic seals.

In particular: see REQ 7.15-02 to 7.15-04

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 5-01 for details.

[REQ 7.15-02] The VA shall provide evidence on how it meets the applicable legal requirements. Including, in particular, eIDAS' regulation of qualified trust services, including any standards specified by the Commission, cf. [eIDAS] article 19 4.a).

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 8.4-05 for details.

[REQ 7.15-03] Services and end user products provided by the VA shall be made accessible for persons with disabilities, where feasible and applicable standards on accessibility such as [ETSI EN 301 549[should be taken into account.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9-03 for details.

[REQ 7.15-04] Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This requirement is implemented according to certificate policies by qualified trust service provider. See CPS REQ 9.4.1-01 for details.