Public policy for qualified signature and seal validation

Version 1.0

28 August 2020

Contents

1. INTRODUCTION

1.1 Introduction

If you want to trust electronic signatures or electronic seals, it is important to have a trustworthy process in place for validation that features all necessary controls to verify that the electronic signature or the electronic seal was valid at the time of signature. A recipient of data containing electronic signatures or electronic seals may choose to undertake a validation or use a trust service that offers validation of electronic signatures and electronic seals. In accordance with [eIDAS], such a validation service is an electronic trust service and thus subject to the eIDAS regulation of trust services, unless the service is excluded, see article 2. This also means that a validation service can obtain status as a qualified trust service if the requirements for qualified trust services are met.

The overall security for validation of electronic signatures and electronic seals depends on the validation processes as well as the underlying running of the validation service. This validation policy lays down requirements for providers wanting to provide a qualified validation service for validation of electronic signatures and electronic seals, see [eIDAS]. This may be both qualified electronic signatures and seals as well as non-qualified electronic signatures and seals. Providers may choose to use alternative validation policies as long as they meet the requirements of [eIDAS].

This document is created to meet the requirements in [ETSI EN 319 401] and [ETSI 319 102-1].

ETSI offers a number of technical specifications that a VA may choose to incorporate in the VA's validation service. This might make the work easier for the VA, provided that the specifications are subsequently turned into a European code included in future versions of this policy:

- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services
- ETSI TS 119 442 Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services
- ETSI TS 119 102-2 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report

Note that this English version is a courtesy translation, which might not be 100% accurate. In case of doubt, the Danish version should be regarded as the authoritative source.

1.2 Document name

This document titled 'Public policy for qualified signature and seal validation', abbreviated PPQV, describes a public policy for qualified validation of electronic signatures and electronic seals. The most recent version of this policy for validation is available at https://certifikat.gov.dk.

1.3 Policy administration

1.3.1 Organization administering the document

This policy is owned and maintained by the Danish Agency for Digitisation.

1.3.2 Contact person

Inquiries regarding this policy can be addressed to:

The Danish Agency for Digitisation

Landgreven 4

DK-1301 Copenhagen K

Telephone: +45 3392 5200

Email: digst@digst.dk

1.3.3 Policy approval procedure

This policy is approved by the Danish Agency for Digitisation following public consultation.

1.3.4 Publication

[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.

1.4 Intellectual property rights

2. REFERENCES

[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 301 549]	Accessibility requirements suitable for public procurement of ICT products and services in Europe

[ETSI EN 319 102-1]	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation - Version 1.1.1 (2016-05)
[ETSI EN 319 401]	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

3. DEFINITIONS AND ACRONYMS

3.1 Definitions

B signature: A signature or seal that can be validated as long as the corresponding certificates have not been revoked, cf. *Basic signature* defined in clause 4.3.1 of [ETSI 319 102-1].

Public key certificate: An electronic certificate specifying the subscriber's public key as well as additional information which uniquely links the public key to the identification of the subscriber. A public key certificate must be signed by a Certification Authority (CA) which thus confirms the validity of the certificate.

Electronic signature: Data in electronic form, which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

Electronic seal: Data in electronic form which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

LTA signature: A signature or seal with long-term availability and integrity of validation data, see *Signature providing Long Term Availability and Integrity of Validation Material* defined in clause 4.3.1 of [ETSI EN 319 102-1].

LTV signature: A signature or seal with integrated validation data, see *Signature with Long-Term Validation Material* defined in clause 4.3.1 of [ETSI EN 319 102-1].

Signature with time-stamping: A signature or seal with integrated time-stamping, see *Signature with Time* defined in clause 4.3.1 of [ETSI EN 319 102-1].

Validation policy: A set of rules outlining requirements for validation of electronic signatures and/or electronic seals. This document is a validation policy.

Validation Authority (VA): A provider of a trust service for validation of electronic signatures and/or electronic seals, see article 3(16)(a) of eIDAS.

3.2 Abbreviations

AdES 'Advanced Electronic Signature'

BCP 'Business Continuity Plan'

CA 'Certification Authority'

ETSI 'European Telecommunications Standards Institute'

TSL 'Trusted Service List'

UTC 'Universal Time Coordinated'

VA 'Validation Authority'

4. GENERAL CONCEPT DESCRIPTION

4.1 General description of requirements for trust service providers that validate electronic signatures and electronic seals

To ensure a uniform level of security for trust service providers, ETSI has published a number of standards that set out various requirements.

[ETSI EN 319 401] contains general requirements for trust service providers, while [ETSI EN 319 102-1] imposes specific requirements for signature and seal generation as well as signature and seal validation for signatures and seals in AdES format.

4.2 Validation service

A validation service may be used both internally in an organization and as a service to external parties. If the service is provided generally, the provider will typically be a trust service provider regulated by [eIDAS]. A validation service may be qualified see [eIDAS] articles 32 and 33.

In the following, a qualified trust service provider providing a validation service validating electronic signatures or electronic seals will be referred to as a qualified validation authority (abbreviated VA).

The VA may use subcontractors in connection with the service provided, but always holds the overall responsibility for ensuring that the requirements of this policy are met.

4.3 Subscriber

A subscriber is natural or a legal entity, who following agreement with the VA, may have an electronic signature or an electronic seal validated.

If the subscriber is a natural person, the subscriber is directly responsible for complying with the terms and conditions for the use of the service.

If the subscriber is a legal entity, the subscriber is responsible for complying with the terms and conditions for its end-users' use of the service. This means that it is the duty of the subscriber to enforce compliance with terms and conditions for the use of the service towards its end-users. In this context, end-users include natural persons working under an instruction from the subscriber as well as systems with the subscriber that use the VA's services.

4.4 Validation policy and VA practice statement

A validation policy is a Trust Service Policy as defined in [ETSI EN 319 401] that sets out requirements for trust service providers.

A VA practice statement is a Trust Service Practice Statement as defined in [ETSI EN 319 401] which describes how a given VA has implemented the requirements for one or more validation policies.

5. INTRODUCTION TO VALIDATION POLICY AND GENERAL REQUIREMENTS

5.1 General requirement

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

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

5.2 Identification

This policy is identified as 'Public policy for qualified signature and seal validation - Version 1.0'

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.

[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.

[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.

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

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

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.

[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.

[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.

[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.

[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.

[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

Note: As concerns item a) above, the VA may choose to specify a class of root certificates provided that reference is also made to the CA root certificates the class contains. For instance, the VA may specify that the VA's trust anchor consists of all CA root certificates available on the European Commission's TSL.

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

6.3 Terms and conditions

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

[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.

[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.

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

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

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

[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.

[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.

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.

[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.

[REQ 6.4-03] The VA shall communicate changes to the information security policy to relevant parties. This includes subscribers, assessment bodies, supervisory or other regulatory bodies

[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.

[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.

Note: Employees working for the VA's organization but who do not carry out work related to its roles as VA are not covered by the above requirement.

[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.

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

[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.

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

[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.

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

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.

7.2 Internal organization

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

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

[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.

Note: It is possible for the VA to limit the field of operation for its services, and the VA should publish its field of operation in its practice statement. For instance, the VA may specify that validations are solely undertaken for a determined number of subscribers and for electronic signatures and electronic seals for which certificates from a number of specified CAs have been used.

[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.

[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.

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

Note: The above requirements must be assessed in respect of the context in which the VA operates, including but not limited to the number of customers and the financial risk undertaken by the VA in respect of the validated electronic signatures and electronic seals.

[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.

[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.

[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.

7.3 Personnel controls

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

[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.

[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

[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.

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

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

[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.

[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.

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

[REQ 7.3-10] The VA's personnel (both temporary and permanent) shall have job descriptions defined from the view point 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.

[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.

[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.

[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.

[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.

[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.

[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 according to the "least privilege" principle.

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

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.

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.

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:

- **[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.
- **[REQ 7.5-03]** Firewalls shall also be configured to prevent all protocols and accesses not required for the operation of the VA.
- **[REQ 7.5-04]** The VA shall implement an efficient user administration, including administer user access of operators, administrators and system auditors.
- **[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.
- **[REQ 7.5-06]** Access to information and application system functions shall be restricted in accordance with the access control policy.
- **[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.
- **[REQ 7.5-08]** The VA's personnel shall be identified and authenticated before using critical systems and applications.
- **[REQ 7.5-09]** The VA's personnel shall be accountable for their activities., e.g. through efficient event logging.

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.

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.

In particular:

[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.

[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].

[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*

Note: The status may be presented without using the terms TOTAL-PASSED, TOTAL-FAILED and INDETERMINATE as long as it cannot be misunderstood which of the three types the result covers.

[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].

Note: Where relevant, the result may be presented in stages, so that the overall result is presented first, while the technical details are hidden in sub-menus or the like.

Note: There are various ways for the VA to implement the validation, such as:

- running as part of an application software on a device like a PC with a graphical user interface;
- as a web service;
- a web application;

- a command-line tool;
- an SDK or a middleware for other applications.

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.

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.

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.

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].

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].

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].

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].

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.

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

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].

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].

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].

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].

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].

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].

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].

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.

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

[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.

[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.

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

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.

[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.

[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.

[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.

[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.

[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.

[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.

[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.

7.10 Network security

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

In particular:

- **[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.
- **[REQ 7.10-03]** The VA shall apply the same security controls to all systems co-located in the same zone.
- **[REQ 7.10-04]** The VA shall restrict access and communications between zones to those necessary for the operation of the VA.
- **[REQ 7.10-05]** The VA shall explicitly forbid or deactivate not needed connections and services.
- **[REQ 7.10-07]** The VA shall review the established network and firewall rules set on a regular basis.
- **[REQ 7.10-09]** The VA shall place particularly critical systems in high-security zones.
- **[REQ 7.10-10]** The VA shall separate dedicated networks for administration of IT systems and the VA's operational network.
- **[REQ 7.10-11]** The VA shall not use systems used for administration of the security policy implementation for other purposes.
- **[REQ 7.10-12]** The VA shall separate the production systems from systems used in development and testing.
- **[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.
- **[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.
- **[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.
- **[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.

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:

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

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:

- **[REQ 7.12-02]** The VA shall maintain the confidentiality and integrity of archived records concerning operation of its services.
- **[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.
- **[REQ 7.12-04]** Records, including audit log, shall be made available if required for the purposes of providing evidence in legal proceedings.
- **[REQ 7.12-05]** The precise time of significant environmental, key management and clock synchronization events shall be recorded.
- **[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.
- **[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.
- **[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.

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 an disaster.

[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.

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:

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

  Before the VA terminates its services, the following procedures apply:

  a) **[REQ 7.14-03]** 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.
  b) **[REQ 7.14-04]** Before the VA terminates its services, the VA shall make the information of the termination available to other relying parties.

c) **[REQ 7.14-05]** 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.
d) **[REQ 7.14-06]** 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.
e) **[REQ 7.14-07]** 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.
f) **[REQ 7.14-08]** Where possible the VA should make arrangements to transfer provision of trust services for its existing customers and users to another VA.

- **[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.
- **[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.
- **[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.

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:

- **[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).
- **[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.
- **[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.

ANNEX A

The compliance with requirements for qualified validation services of this policy as set out in [ETSI EN 319 401] and [ETSI EN 319 102-1].

QVA	ETSI EN 319 401	ETSI EN 319 102-1
REQ 1.3.4-01		
REQ 5.1-01		
REQ 5.1-02		
REQ 6.1-01	REQ-5-01	
REQ 6.1-02	REQ-5-02	
REQ 6.1-03	REQ-5-03	
REQ 6.1-04	REQ-5-04	
REQ 6.1-05	REQ-5-05	
REQ 6.2-01	REQ-6.1-01 REQ-6.1-03 REQ-6.1-04 REQ-6.1-05	
REQ 6.2-02	REQ-6.1-02 REQ-6.1-06 REQ-6.1-07	
REQ 6.2-03	REQ-6.1-02 REQ-6.1-10	
REQ 6.2-04	REQ-6.1-08 REQ-6.1-09	
REQ 6.2-05	REQ-6.1-11 REQ-7.12-10	
REQ 6.2-06		
REQ 6.2-07		
REQ 6.3-01	REQ-6.2-01	
REQ 6.3-02	REQ-6.2-02	
REQ 6.3-03	REQ-6.2-03	
REQ 6.3-04	REQ-6.2-04	
REQ 6.3-05	REQ-6.2-05	
REQ 6.3-06	REQ-6.2-06	
REQ 6.3-07		
REQ 6.3-08		
REQ 6.4-01		
REQ 6.4-02	REQ-6.3-01	
REQ 6.4-03	REQ-6.3-02	
REQ 6.4-04	REQ-6.3-03	
REQ 6.4-05	REQ-6.3-04	
REQ 6.4-06	REQ-6.3-05	
REQ 6.4-07	REQ-6.3-06	
REQ 6.4-08	REQ-6.3-07	
REQ 6.4-09	REQ-6.3-08	

REQ 6.4-10	REQ-6.3-09	
REQ 6.4-11	REQ-6.3-10	
REQ 7.1-01		
REQ 7.2-01		
REQ 7.2-02	REQ-7.1.1-01 REQ-7.1.1-02	
REQ 7.2-03	REQ-7.1.1-03	
REQ 7.2-04	REQ-7.1.1-04	
REQ 7.2-05		
REQ 7.2-06	REQ-7.1.1-05	
REQ 7.2-07	REQ-7.1.1-06	
REQ 7.2-08	REQ-7.1.1-07	
REQ 7.2-09	REQ-7.1.2-01	
REQ 7.3-01	REQ-7.2-01	
REQ 7.3-02		
REQ 7.3-03	REQ-7.2-03	
REQ 7.3-04	REQ-7.2-02	
REQ 7.3-05	REQ-7.2-04	
REQ 7.3-06	REQ-7.2-05	
REQ 7.3-07	REQ-7.2-06	
REQ 7.3-08	REQ-7.2-07 REQ-7.2-08	
REQ 7.3-09	REQ-7.2-09	
REQ 7.3-10	REQ-7.2-10	
REQ 7.3-11	REQ-7.2-11	
REQ 7.3-12	REQ-7.2-12	
REQ 7.3-13	REQ-7.2-13	
REQ 7.3-14	REQ-7.2-14	
REQ 7.3-15	REQ-7.2-15	
REQ 7.3-16	REQ-7.2-16	
REQ 7.3-17	REQ-7.2-17	
REQ 7.4.1-01	REQ-7.3.1-01 REQ-7.3.1-02	
REQ 7.4.2-01	REQ-7.3.2-01 REQ-7.4-10 REQ-7.7-06	
REQ 7.5-01	REQ-7.4-01	
REQ 7.5-02	REQ-7.4-02	
REQ 7.5-03	REQ-7.4-03	
REQ 7.5-04	REQ-7.4-04	
REQ 7.5-05	REQ-7.4-05	
REQ 7.5-06	REQ-7.4-06	
REQ 7.5-07	REQ-7.4-07	
REQ 7.5-08	REQ-7.4-08	
REQ 7.5-09	REQ-7.4-09	
REQ 7.6.1-01	REQ-7.5-01	

REQ 7.7.1-01		ETSI EN 319 102-1 clause 5.1.1
REQ 7.7.1-02		ETSI EN 319 102-1 clause 5.1.1
REQ 7.7.1-03		ETSI EN 319 102-1 clause 5.1.1
REQ 7.7.1-04		ETSI EN 319 102-1 clause 5.1.1
REQ 7.7.1-05		ETSI EN 319 102-1 clause 5.1.1
REQ 7.7.2-01		ETSI EN 319 102-1 clause 5.1.2
REQ 7.7.3-01		ETSI EN 319 102-1 clause 5.1.3
REQ 7.7.4-01		ETSI EN 319 102-1 clause 5.1.4
REQ 7.7.5-01		ETSI EN 319 102-1 clause 5.2.2
REQ 7.7.6-01		ETSI EN 319 102-1 clause 5.2.3
REQ 7.7.7-01		ETSI EN 319 102-1 clause 5.2.4
REQ 7.7.8-01		ETSI EN 319 102-1 clause 5.2.5
REQ 7.7.9-01		ETSI EN 319 102-1 clause 5.2.6
REQ 7.7.9-02		
REQ 7.7.10-01		ETSI EN 319 102-1 clause 5.2.7
REQ 7.7.11-01		ETSI EN 319 102-1 clause 5.2.8
REQ 7.7.12-01		ETSI EN 319 102-1 clause 5.2.9
REQ 7.7.13-01		ETSI EN 319 102-1 clause 5.3
REQ 7.7.14-01		ETSI EN 319 102-1 clause 5.4
REQ 7.7.15-01		ETSI EN 319 102-1 clause 5.5
REQ 7.7.16-01		ETSI EN 319 102-1 clause 5.6
REQ 7.8-01	REQ-7.6-01	
REQ 7.8-02	REQ-7.6-02	
REQ 7.8-03	REQ-7.6-03 REQ-7.6-04	
REQ 7.8-04	REQ-7.6-05	
REQ 7.8-11		
REQ 7.9-01	REQ-7.7-01	
REQ 7.9-02	REQ-7.7-02	
REQ 7.9-03	REQ-7.7-03 REQ-7.7-04	
REQ 7.9-04	REQ-7.7-05 REQ-7.7-09	
REQ 7.9-05	REQ-7.7-06	
REQ 7.9-06	REQ-7.7-07	
REQ 7.9-07	REQ-7.7-08	
REQ 7.9-08		
REQ 7.10-01	REQ-7.8-01	
REQ 7.10-02	REQ-7.8-02	
REQ 7.10-03	REQ-7.8-03	
REQ 7.10-04	REQ-7.8-04	
REQ 7.10-05	REQ-7.8-05	
REQ 7.10-07	REQ-7.8-06	
REQ 7.10-09	REQ-7.8-07	
REQ 7.10-10	REQ-7.8-08	
REQ 7.10-11	REQ-7.8-09	

REQ 7.10-12	REQ-7.8-10	
REQ 7.10-13	REQ-7.8-11	
REQ 7.10-14	REQ-7.8-12	
REQ 7.10-15	REQ-7.8-13	
REQ 7.10-16	REQ-7.8-14 REQ-7.8-15	
REQ 7.11-01	REQ-7.9-01	
REQ 7.11-02	REQ-7.9-02	
REQ 7.11-03	REQ-7.9-03	
REQ 7.11-04	REQ-7.9-04	
REQ 7.11-05	REQ-7.9-05	
REQ 7.11-06	REQ-7.9-06	
REQ 7.11-07	REQ-7.9-07	
REQ 7.11-08	REQ-7.9-08	
REQ 7.11-09	REQ-7.9-09	
REQ 7.11-10	REQ-7.9-10	
REQ 7.11-11	REQ-7.9-11	
REQ 7.11-12	REQ-7.9-12	
REQ 7.12-01	REQ-7.10-01	
REQ 7.12-02	REQ-7.10-02 REQ-7.10-08	
REQ 7.12-03	REQ-7.10-02 REQ-7.10-03	
REQ 7.12-04	REQ-7.10-04	
REQ 7.12-05	REQ-7.10-05	
REQ 7.12-06	REQ-7.10-06	
REQ 7.12-07	REQ-7.10-07	
REQ 7.12-08	REQ-7.10-02 REQ-7.10-08	
REQ 7.13-01	REQ-7.11-01	
REQ 7.13-02	REQ-7.11-02	
REQ 7.14-01	REQ-7.12-01	
REQ 7.14-02	REQ-7.12-02	
REQ 7.14-03	REQ-7.12-03	
REQ 7.14-04	REQ-7.12-04	
REQ 7.14-05	REQ-7.12-05	
REQ 7.14-06	REQ-7.12-06	
REQ 7.14-07	REQ-7.12-07	
REQ 7.14-08	REQ-7.12-08	
REQ 7.14-09	REQ-7.12-11	
REQ 7.14-11	REQ-7.12-09	
REQ 7.14-12	REQ-7.12-10	
REQ 7.15-01	REQ-7.13-01	
REQ 7.15-02	REQ-7.13-02	
REQ 7.15-03	REQ-7.13-03 REQ-7.13-04	

REQ 7.15-04	REQ-7.13-05	