CERTIFICATION PRACTICE STATEMENT FOR DPDSA SERVER CERTIFICATES FOR THE SOCIAL WELFARE AND HEALTHCARE SECTOR

OID: 1.2.246.517.1.10.208.1

15.9.2023

Document management	
Owner	
Prepared by	Tuire Saaripuu
Inspected by	
Approved by	Mikko Pitkänen

Version control		
version no.	what has been done	date/person
v 1.0	Approved version 1.0	3.5.2018
v.1.1	Updated version	18.6.2019
v 1.2	Updated version, Centre name change.	1.1.2020
v 1.3	Updated version, accessibility features, updated name of the act 661/2009	6.5.2021
v 1.4	Added information regarding ETSI QCP-w, Added information regarding ETSI QCP-w, changed the maximum issuance time of certificates, added information regarding CA:s responsibility on checking registrar's domain	1.10.2021/VA
v 1.5	Updated version and CPS links	22.9.2022/SK
v 1.6	Updated version	15.9.2023/MK

Table of contents

1 General points 5

2 List of references 5

2.1 Reference documents 5

2.2 References for additional information 6

2.3 Definitions 6

2.4 Acronyms 8

3 Common concepts 9

3.1 Certification authority 9

3.2 Certificate Services 11

3.2.1 Registration authority 11

3.2.2 Revocation service 12

Directory service 12

1. Certificate policy and certification practice statement 12

3.2.3 Purpose 12

3.2.4 Level of detail 12

3.2.5 Approach 12

3.2.6 Other documents published by the certification authority 12

2. Customer and signatory 13

4 Introduction to certificate policy documents 13

4.1 General points 13

4.2 Unique identifiers 14

4.3 User community and applicability 14

4.4 Compliance 14

4.4.1 General points 14

4.4.2 Compliance requirements 15

5 Responsibilities, liabilities and limitations of liabilities 16

3. Certification authority's responsibilities 16

4. Responsibilities of the customer and certificate holder 17

5. Responsibilities of the party relying on a certificate 18

6. Responsibilities and limitations of liability 18

7. Requirements applicable to the operation of the certification authority 20

8. Certification practice statement 21

9. Life cycle management of keys used in a public key infrastructure 21

5.1.1 Creation of certification authority’s keys 21

5.1.2 Storage, backup and recovery of the certification authority's key 22
5.1.3 Distribution of the certification authority's public key 22
5.1.4 Backup key system 23
5.1.5 Use of the certification authority's key 23
10. Life cycle management of certificates used in a public key system 23
5.1.6 Signatory registration 23
5.1.7 Renewing a certificate, changing the key pair and updating a certificate 25
5.1.8 Creation of certificates 26
5.1.9 Distribution of terms of use 27
5.1.10 Distribution of certificates 28
5.1.11 Revoking a certificate and placing it in a suspended state 28
11. The certification authority's management and operating procedures 31
5.1.12 Security management 31
5.1.13 Repository classification and management 31
5.1.14 Staff and information security 31
5.1.15 Physical security and security of the environment 33
5.1.16 Operations management 33
5.1.17 Management of access to systems 34
5.1.18 Commissioning and maintenance of systems to be trusted 34
5.1.19 Business continuity management and processing of anomalies 34
5.1.20 End of the certification authority's operation 35
5.1.21 Applicable legislation 36
5.1.22 Retention of information pertaining to certificates 36
12. Organisation requirements 37
13. . Framework for the specification of other certificate policy documents 38
14. Specification document management 39
15. Additional requirements 39
16. Compliance 40

CERTIFICATION PRACTICE STATEMENT FOR DPDSA SERVER CERTIFICATES FOR THE SOCIAL WELFARE AND HEALTHCARE SECTOR

1 General points

This document defines the prerequisites of the PKI (Public Key Infrastructure) certification activities of the Digital and Population Data Services Agency (hereinafter 'the certification authority') and the scope of application and limitations of this document. At practical level, the principles contained in this document are laid out, in addition to this certification practice statement, in other procedural guidelines supplementing this document.This document complies with ETSI TS 102 042 v2.1.2:n (LCP) policies regarding the service certificate.

The status and tasks of the Certification Authority have been established by the Act on the Digital and Population Data Services Agency (304/2019), previously knowns as Population Register Centre.

The server certificates described in this certificate practice statement adhere to the ETSI QCP-w (0.4.0.194112.1.4) certificate policy for European Union (EU) qualified website authentication certificates.

2 List of references

2.1 Reference documents

The certification authority's PKI has been formulated on the basis of the following statutes, standards and guidelines:

[1] Act on Strong Electronic Identification and Trust Services (617/2009)

[2] Act on Electronic Services and Communication in the Public Sector (13/2003)

[3] The Act on the Openness of Government Activities (621/1999)

[4] IETF RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (11/2003)

[5] ETSI TS 102 042 V2.1.2: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (2010-04)

[6] Finnish Transport and Communications Agency regulations, Finnish Communications Regulatory Authority 7 B/2009 M

[7] Finnish Communications Regulatory Authority 8 B/2009 M

[8] VAHTI 5/2004: Securing the state administration's key information systems

[9] ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management.

[10] Guidelines for The Issuance and Management of Extended Validation Certificates, CA Browser Forum, 1 October 2009, Version 1.2.

The following principles apply to the interpretation of this document:

1. The headings and subheadings of the certificate policy are primarily recommendations of international standards [RFC 3647] which have been translated into Finnish. When interpreting this document, the body of the text takes precedence over the headings

2. As a general condition, all requirements concerning the certification authority as set out in this certification practice statement must be fulfilled.

2.2 References for additional information

While the references listed below are not essential for using this document, they will provide the user with support on certain topics. In the absence of an accurate reference, the most recent version of the document should be used (including revisions).

[i.1] 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.

2.3 Definitions

Attribute data: data of permanent nature required to identify a professional and to verify his or her professional practice rights.

Key pair: A pair of interconnected keys, one public and one private, which are used in public key methods. The purpose of the keys is defined in the certificate. NB: See also section 4.3

Asymmetric encryption: A pair consisting of one public key and one private key is used in asymmetric encryption. A message that has been encrypted using a public key can only be accessed by the private key of the key pair in question.

Certificate policy applied to Extended Validity (EV) certificates: normalised certificate policy (NCP) expanded to comply with the EVCG [11] instructions.

Directory service: A public Internet-based service which can be used to retrieve all certificates issued by the certification authority as well as CA certificates and revocation lists.

Public key: The public component of a key pair used in asymmetric encryption in public key methods. The certification authority certifies with its electronic signature that the public key belongs to the certificate holder. The public key is part of the data content of the certificate.

Public key infrastructure: An information security infrastructure in which security services are provided by public key methods.

Public key method: An information security service, such as electronic identification of a person, which is provided using public and private keys, certificates and asymmetric encryption.

Relying party: A party that trusts the certificate data and uses the certificate for various information security services, such as electronic identification of the certificate holder and authentication of a digital signature. NB: See RFC 3647

Server certificate: A service certificate used to identify a server and to generate an SSL/TLS encrypted connection between servers. For example, a certificate intended for a www server that allows the user to verify that the server can be trusted. A dataset consisting of the public key and identification data of a party using the PKI that has been created and signed by the certification authority using its private key.

Server certificate for e-service use: A file-based certificate intended for such purposes as receiving and sending encrypted e-mails using a shared mailbox. The file contains both the certificates and the associated private and public key.

Service certificate: A term that covers both server and e-mail service certificates.

Registration authority: The registration authority identifies the certificate applicant in accordance with the certificate policy and certification practice statement on behalf of and at the responsibility of the certification authority.

RSA algorithm and RSA key: The RSA algorithm is a common public key algorithm. The private and public keys associated with a service certificate are RSA keys.

A protected user device: a device that stores the user’s private key, protects the key from being compromised and performs signature or decryption functions for the user.

Revocation list (CRL): A list of certificates revoked before the end of their validity period and the revocation dates, electronically signed and published by the certification authority. The revocation list specifies the publication dates of the current and next revocation list. Revoked certificates are added to the list. NB: See ITU-T Recommendation X.509.

Revocation service: A certification authority's service that receives certificate revocation requests, revokes the certificates and communicates the fact that the certificate has been revoked to the certificate system.

An electronic signature: a PKI signature attached to an electronic message that enables the reliable authentication of the message contents and the signatory’s identity.

Certificate: A digital certificate that associates the signature authentication data with the signatory and authenticates the signatory. A certificate contains an OID (object identifier) that identifies the certification practice statement in question.

Certificate system: An IT system used to create certificates, sign revocation lists and publish the lists in a directory.

PKI disclosure statement: A document that contains the main points of the certificate policy and certification practice statement.

Certificate policy: A document that describes the principles of certification and the responsibilities of the relying parties. The certificate policies published by the DPDSA are publicly available. Each certificate policy is identified by an OID.

Certificate management system: A data system consisting of certificate systems, data communications, a certificate directory, a revocation list service, an advice and revocation service, certificate management and card management.

CPS OID is part of the data content of the certificate.

Certification practice statement: A description of how the certification authority implements its certificate policy. Each certification practice statement is identified by an OID.

Certification authority: An organisation that issues certificates, is responsible for their creation and draws up a certificate policy that describes its operation and the associated certification practice statement. NB: See section 4.1

CA certificate: Contains the name, country and public key of the certification authority.

Certification authority's private key: The private key used by the certification authority to sign the certificates it issues and the revocation lists it publishes.

Certificate applicant: An organisation or an individual who applies for a certificate and that is reliably identified at the time of submitting the application.

Certificate holder: An organisation or an individual whose data and public key are verified by the certification authority's digital signature and who holds the private key linked with the certificate in question.

Certificate usage and purpose: In this document, certificate usage refers to the use of both the certificate and the associated keys. For example, using a certificate to create an electronic signature refers to both the use of a private key for signing a document and to the use of the public key and certificate for verifying the signature.

Private key: The private component of a key pair used in asymmetric encryption in public key methods. The certificate holder’s private key is stored in a safe environment to protect it from unauthorised use.

2.4 Acronyms

CA Certification Authority

CP Certificate Policy

CPS Certification Practise Statement

CRL Certificate Revocation List

CSP Certification Service Provider

EVC Extended Validity Certificate

EVCP Extended Validity Certificate Policy

FINEID Finnish Electronic Identification

HSM Hardware Security Module

HTTP Hypertext Transfer Protocol

ISO 27001, ISO/IEC 27001

LCP Lightweight Certificate Policy

LDAP Lightweight Directory Access Protocol

OID Object Identifier

PDS PKI Disclosure Statement

PKI Public Key Infrastructure

RSA Rivest, Shamir, Adleman, a public key algorithm, an asymmetric algorithm

SSL Secure Socket Layer

TLS Transport Layer Security

DPDSA Digital and Population Data Services Agency

3 Common concepts

3.1 Certification authority

A certification authority is a party that issues and creates certificates trusted by the certificate service users (customers and parties relying on the certificate). The certification authority has overall responsibility for the provision of the certificate services defined in section 4.2. The certification authority is identified in the certificate as the issuer of the certificate, and its public key is used to sign qualified certificates.

The certification authority may use third parties in its provision of certificate services to provide parts of the service. However, the certification authority will always carry the overall responsibility and ensure that the procedural requirements set forth in this document are met. The certification authority may, for example, outsource all components of the service, including the certificate creation service. However, the key used for signing the certificates will be defined as belonging to the certification authority, and the certification authority retains overall responsibility for meeting the requirements specified in this document and the responsibility for issuing certificates to be granted to the public.

The certification authority is a certification service provider issuing certificates to the public.

The certification authority meets the following terms and conditions:

- The certification authority agrees to adhere to the terms and conditions set out in the certificate policy.
- The certification authority prepares a certificate practice statement and other procedural instructions that complement the certificate policy.
- The certification authority maintains adequate financial resources in order to secure the operations referred to in this certificate policy. The certification authority is responsible for the certificate activities and the associated risks and requires the certificate system suppliers to take appropriate risk management measures in order to safeguard against risks related to the activities.
- The certification authority maintains a register of its approved registration authorities.
- The certification authority makes decisions on cross-certification in co-operation with other certification authorities.
- The certification authority is responsible for the life cycle of key pairs created by it (generation, storage, backups, publishing and disposal) and for publishing the revocation lists.

The certification authority agrees to:

1. offer the certificate, directory and revocation services specified in the certificate policy;
2. provide the management and monitoring functions described in sections 4–6 of this certification practice statement;
3. reliably identify certificate applicants;
4. issue certificates in accordance with this certification practice statement;
5. comply with valid acts and decrees as well as any regulations and guidelines issued by virtue of them, and support the rights of certificate users and relying parties;
6. ensure that sufficient independent auditing is performed in accordance with the certification practice statement;
7. ensure the functioning of the certification authority; and
8. comply with all terms and conditions in the certificate policy and this certification practice statement.

The certification authority may, at its discretion, offer additional functions or services related to the certificate system.

The certification authority is responsible for ensuring that information contained in the certificate is in accordance with this certification policy statement.

3.2 Certificate Services

3.2.1 Registration authority

Registration authorities who operate under this certificate policy must meet the following terms and conditions:

- The registration authority agrees to comply with the requirements set out in this certification practice statement.
- The registration authority must be approved and registered by the certification authority.
- The registration authority is responsible for the identification of certificate applicants.
- The registration authority is responsible for the trustworthiness of the registration point personnel. The registration authority obtains background checks on recruited personnel as required by the certification authority and ensures the trustworthiness of its personnel at all times. The certification authority approves the registration point personnel on the basis of background checks obtained by the registration authority.

A registration authority operating under this certificate policy must agree to:

1. comply with valid legislation as well as the regulations and guidelines issued by virtue of it;
2. provide the management and monitoring functions specified in sections 4–6 of this certification practice statement;
3. complete an identification procedure on certificate applicants as described in Chapters 4–6 of this certification practice statement and the certificate policy as well as submit the applicant's data to the certification authority for the purpose of creating the certificate;
4. perform the agreed assignments and support the rights of certificate users and relying parties; and
5. comply with all terms and conditions related to the registration service in the certificate policy and this certification practice statement.

The registration authority may offer additional functions or services approved by the certification authority. The registration authority is responsible for all registration services provided by it. The registration authority for the service certificate is the Digital and Population Data Services Agency.

3.2.2 Revocation service

The certificate revocation service revokes service certificates that the certificate holder or the certification authority wishes to revoke before their stipulated expiry date. Revoked service certificates are added to the revocation list. Reasons for revoking service certificates may include knowing or suspecting that the certificate holder's private key has been compromised.

Directory service

The directory service is a public Internet-based service which can be used to retrieve all service certificates issued by the certification authority as well as CA certificates and revocation lists. The directory service is available at ldap://ldap.fineid.fi.

1. Certificate policy and certification practice statement

3.2.3 Purpose

A certificate policy is a document drawn up by a certification authority (CA) which describes the practices and principles used in certification. The certification practice statement is a more detailed description of the certification authority's activities than a certificate policy.

3.2.4 Level of detail

The certification practice statement describes in more detail than the certificate policy the practices the certification authority follows in issuing certificates and other administration. It specifies how a certain certification authority meets the technical, organisational and procedural requirements specified in the certificate policy.

3.2.5 Approach

The approaches of the certificate policy and the certification practice statement are completely different. A certificate policy is formulated independently of the details in a certain certification authority's operating environment. A certification practice statement, on the other hand, is specifically prepared to match the certification authority's organisation structure, operating methods, facilities and ICT environment. The certificate policy may be defined by a certificate service user, while the certification practice statement is always specified by the certificate provider.

3.2.6 Other documents published by the certification authority

In addition to the certificate policy and certification practice statement, the certification authority may publish other documents pertaining to its certification activities. Such terms and conditions of use may contain many types of commercial terms or, among other things, be associated with a certain PKI. Even if the customer is not necessarily informed of these terms, they may still become applicable.

The PKI disclosure statement is part of the certification authority's terms of use related to the functionality of the public key system. The certification authority should make the PKI disclosure statement available for both the customers and the relying parties.

2. Customer and signatory

A “customer” refers to a party that applies to the certification authority for certificates and that has a contractual relationship with the certification authority (an organisation or an individual). A “signatory” refers to the party to which the certificate was issued (an organisation or an individual). The customer is responsible for the use of a private key associated with a certificate based on a public key. The signatory, on the other hand, is a person who can be authenticated using a private key and who controls the private key's use.

When certificates are issued to individuals for their private use, the same person may be both a customer and a signatory. In other cases, as when certificates are issued for employees, the customer and the signatory are different parties. For example, an employer may be the customer, while an employee is the signatory.

These two concepts are used in this document to make this distinction whenever necessary. In all cases, however, the difference is not quite clear.

4 Introduction to certificate policy documents

4.1 General points

A certificate policy is a document drawn up by a certification authority (CA) which describes the practices and principles used in certification. The certification practice statement is a more detailed description of the certification authority’s activities than a certificate policy.

The certification practice statement is applied to the Digital and Population Data Services Agency’s service certificates. The service certificate is a certificate granted by the Digital and Population Data Services Agency used to authenticate a service provider’s service or server.

A certificate is a dataset that, in connection with authentication or encryption, links the authentication data to the certificate holder and authenticates the service certificate holder. The certificate data are signed electronically by the certification authority's private key. Certificates referred to in this certification practice statement are based on a public key infrastructure (PKI).

Server certificates can be used to authenticate both public administration and private sector services. The server certificate allows the service user to verify the authenticity of the service provider.

The Digital and Population Data Services Agency’s certification practice has a unique identifier (OID). The certification authority's activities include the provision of certification, directory and revocation services as well as registration. For a more detailed description of these activities, see section 4.2.

4.2 Unique identifiers

A certificate contains two unique identifiers (OIDs). One of them indicates the ETSI TS 102 042 Certificate Policy that the certificate complies with, and the other identifies the certification practice statement.

A certificate policy is defined by a unique identifier issued by the DPDSA.

These unique identifies are:

The OID of the ETSI TS 102 042 policy to be complied with (OVCP): 0.4.0.2042.1.7 [itu-t(0), identified-organization(4), etsi(0), other-certificate-policies(2042), policy-identifiers(1), ovcp (7)].

The Digital and Population Data Services Agency’s server certificates for the Social Welfare and Healthcare Sector, certification practice statement OID:1.2.246.517.1.10.208.1.

OID for the DPDSA service certificate for the Social Welfare and Healthcare Sector, certificate policy: 1.2.246.517.1.10.208.

For the certificate policy, its PKI disclosure statement and the certification practice statements, visit https://dvv.fi/en/certificate-policy.

4.3 User community and applicability

The purposes of the server certificate referred to in this Certification Practice Statement include identifying a server and encrypting data communications. The certificate can be used without limitation according to its purpose in administrative applications and services and those provided by private individuals.

The certificate policy and certification practice statement contain requirements concerning the obligations of the certification authority, registration authority, certificate holder and relying party as well as matters related to legislation and dispute resolution.

4.4 Compliance

4.4.1 General points

The certification authority provides certificate services on the terms and conditions set out in the certification practice statement document and assumes responsibility for their functioning. The certification authority is responsible for the functioning of the certificate system as a whole, including on behalf of any registration authorities and technical suppliers it may use. This certification practice statement was registered by the Digital and Population Data Services Agency. The certificate policy documents are published at https://dvv.fi/en/certificate-policy, where they can be accessed by anyone. The certification authority's operation is audited every year and whenever significant modifications have been made in the system. Certificate audit reports are available on request.

Information security audit

The DPDSA carries out information security audits on the facilities, equipment and operations of its technical suppliers as appropriate.

The Digital and Population Data Services Agency’s information security audits are carried out by a third-party auditor who is independent of the certification authority.

The objects of the audit are determined by the Act on Strong Electronic Identification and Trust Services (617/2009) or, if the Digital and Population Data Services Agency is carrying out the audit, information security standard ISO 27001, the Digital and Population Data Services Agency’s information security policy or the technical terms of delivery. Audited information security properties include confidentiality, integrity and availability.

In the audit, the certificate policy, the certification practice statement, the application instructions and their compatibility with ETSI TS 102 042 standard are compared regarding the entire certificate organisation and system.

Measures resulting from deviations

Observed deviations are recorded in the audit report and responded to in accordance with legislation, information security standard ISO 27001 and the valid terms of delivery.

Communicating the result of an audit

The results of an audit are communicated according to the law, information security standard ISO 27001, the Digital and Population Data Services Agency's information security policy and the valid terms of delivery. A detailed, standard form audit result report intended for internal use is confidential and will not be disclosed to the public. Standard form reports are prepared separately for external use.

Archival of the audit documents

The certification authority shall archive the audit reports and records, including information security audits and system audits. The archive data are stored in accordance with regulations pertaining to the certification authority in question.

For a description of the plans and policies concerning the certification authority's operation and the certification authority’s obligations in case of emergencies and disruptions, see section 7.4.8., Continuity management and handling of deviations.

4.4.2 Compliance requirements

For the certification authority’s obligations, see section 6.1. The certification authority's operations meet the requirements set out in section 6.1. The certification authority's operations and their supervision also meet the requirements set out in section 7.

5 Responsibilities, liabilities and limitations of liabilities

3. Certification authority's responsibilities

The certification authority is responsible for the functioning of the certificate system as a whole, including on behalf of any registration authorities and technical suppliers it may use.

- The Digital and Population Data Services Agency is a statutory certification authority.
- The certification authority shall act in compliance with current legislation.
- The certification authority shall perform its duties carefully, reliably and appropriately.
- The certification authority shall have the necessary technical ability and financial resources for appropriately arranging the certificate activities and for covering potential liability for damages.
- The certification authority is responsible for all areas of the certification activity, including the reliability and functioning of the services and products produced by any technical suppliers or persons who assist the certification authority.
- The certification authority draws up and maintains a certificate policy which describes at a general level the procedures for the issuance, maintenance and management of service certificates, the terms and conditions, allocation of responsibilities, and other matters related to the use of service certificates.
- The certification authority draws up and maintains certification practice statements which describe how the certification authority applies its certificate policy.
- The certification authority complies with the certificate policy and certification practice statement requirements.
- The certification authority makes the certificate policy and the certification practice statement publicly available.
- The certification authority shall employ sufficient staff with the expertise, experience and competence required for producing certificate services.
- The certification authority shall use reliable systems and products protected against unauthorised use.
- The certification authority shall keep publicly available information regarding its certificates and certificate activities, based on which the operation and reliability of the certification authority can be assessed.

The registration authority's responsibilities

The registration authority for the service certificate is the Digital and Population Data Services Agency.

- The registration authority shall comply with the certificate policy and the certification practice statement in its registration activities.
- The registration authority identifies the service certificate applicant reliably as described in the certification practice statement, ensuring that the applicant's identity, right to apply for a service certificate and other data related to the applicant necessary for issuing a service certificate are carefully verified.
- The registration authority shall see to the careful handling and confidentiality of the data.
- The registration authority shall adhere to registration procedures agreed upon with the certification authority.

4. Responsibilities of the customer and certificate holder

- The service certificate holder is responsible for ensuring that the certificate is used in compliance with the purposes indicated in the service certificate application, the certificate policy, the certification practice statement and the contractual terms that are binding to the certificate holder.
- The certificate holder (service provider) is responsible for ensuring that the data provided in the application for the certificate are correct.
- The certificate holder must store their private key in a secure environment and make every effort to prevent its loss, disclosure to outsiders, modification or unauthorised use.
- The certificate holder must notify the certification authority immediately if it knows or suspects that the certificate holder's private key has been compromised or that there are errors in the certificate's data content. The certification authority will then revoke the certificate in question, and the relevant private key can no longer be used to produce a new certificate.
- A service certificate holder's responsibility for certificate use ends when they have reported the necessary data to the certification authority and when they have received a revocation notice from the person receiving the call. In order to terminate the liability, the revocation request must be made immediately upon noticing the reason for making the request.

All service certificates that are valid and have been issued using the exposed key must be revoked on one or several revocation lists whose validity period does not expire until the validity of the last revoked service certificate has expired.

If the private key used by the Digital and Population Data Services Agency in certificate creation or another technical method has become exposed or otherwise unusable, the Digital and Population Data Services Agency must duly notify all certificate holders and the Finnish Transport and Communications Agency of this.

A service certificate applicant shall submit to the registration authority a certificate request generated with their server to be certified, and the service certificate will be created on the basis of this request.

The certification authority's private key, which is used to sign service certificates, and the corresponding public key are 4096-bit RSA keys.

The lengths of the private and public key of the service certificate are up to the certificate applicant. The key length of a service certificate issued by the Digital and Population Data Services Agency is 4,096 bits at minimum.

5. Responsibilities of the party relying on a certificate

It is the responsibility of the party relying on a service certificate to ensure that the certificate is used according to its intended use.

A party relying on the service certificate must adhere to the certificate policy and certification practice statement.

A party relying on a service certificate may trust the service certificate in good faith after verifying that the certificate is valid and that it is not on a revocation list. A party relying on a service certificate shall check that the certificate is not on the revocation list. In order to reliably verify the validity of a service certificate, the party relying on the service certificate must comply with the following procedure for revocation list checks.

If a party relying on the service certificate downloads the revocation list from a directory, it must verify the authenticity and integrity of the revocation list by checking the list's electronic signature. In addition, the validity period of the revocation list must be checked.

If the most recent revocation list cannot be retrieved from the directory because of hardware or directory service malfunction, no certificate should be accepted if the validity period of the last retrieved revocation list has expired. All certificates are accepted after the validity period at the risk of the party relying on the certificate.

6. Responsibilities and limitations of liability

Certification authority's responsibilities

The Digital and Population Data Services Agency complies with the valid Finnish legislation in its certificate service activities.

The Digital and Population Data Services Agency as a certification authority is liable for the safety of the entire certificate system. The certification authority is liable for services it has commissioned as if for its own.

The Digital and Population Data Services Agency ensures that service certificates are created in accordance with the procedures defined in the certificate policy and the certification practice statement and according to the data provided by the certificate applicant. The Digital and Population Data Services Agency is only responsible for the data it has stored in the service certificate.

The Digital and Population Data Services Agency's liability related to the provision of certificate services is determined under the valid cooperation agreements and pursuant to the provisions in the Tort Liability Act (412/1974). In addition, the requirements laid down in the Act on Strong Electronic Identification and Trust Services (617/2009) apply to the Digital and Population Data Services Agency.

The Digital and Population Data Services Agency ensures that the service certificate will be available from the time it is handed over for its entire period of validity, unless it has been reported to the revocation list.

The Digital and Population Data Services Agency ensures that the service certificate has been handed over to an applicant identified as required when issuing service certificate.

When signing a service certificate with its private key, the certification authority assures it has checked the data in the certificate following the procedures described in the service certificate policy and the certification practice statement.

The certification authority ensures that the right service certificate is put on the revocation list and that it appears on the revocation list in the time specified in the certification practice statement.

Registration authority's responsibilities

The registration authority of the service certificate is the Digital and Population Data Services Agency or its contracting partner under the responsibility of and contracted by the Digital and Population Data Services Agency.

Certificate holder's responsibilities

The service certificate holder is responsible for ensuring that the certificate is used in compliance with the purposes indicated in the service certificate application.

A service certificate holder's responsibility for certificate use ends when they have reported the necessary data to the certification authority and when they have received a revocation notice from the person receiving the call. In order to terminate the liability, the revocation request must be made immediately upon noticing the reason for making the request.

Responsibilities of a party relying on a certificate

A party relying on a service certificate may not trust the correctness of a certificate in good faith if the validity of the certificate has not been checked against the revocation list. Accepting a service certificate in the above cases releases the Digital and Population Data Services Agency from liability. A party relying on a service certificate shall verify that the issued certificate corresponds to its intended use in the legal action in which it is used.

Limitations of liability

The Digital and Population Data Services Agency is not liable for damages and costs caused by the disclosure of a certificate holder's private key unless the disclosure is the direct result of the Digital and Population Data Services Agency's actions.

The maximum extent of the Digital and Population Data Services Agency's liability to the certificate holder and a relying party is any direct damage incurred, if the damage is the result of the Digital and Population Data Services Agency's direct actions, however at most 15% of the amount invoiced for the certificates over the preceding 3 months (share payable to the DPDSA).

The Digital and Population Data Services Agency is not liable for indirect or consequential damage caused to the certificate holder. Neither is the Digital and Population Data Services Agency liable for indirect or consequential damages incurred by other partners of the relying party or the certificate holder.

The Digital and Population Data Services Agency is not responsible for the operation of public telecommunications, such as the Internet, or for the inability to execute a transaction because of the non-functionality of a device or software used by the service certificate holder, or for the use of a service certificate in contradiction to its intended use.

The certification authority has the right to develop the certificate service. A certificate holder or a relying party must bear their own expenses thus incurred, and the certification authority is not liable to compensate the certificate holder or a relying party for any expenses caused by the certification authority's development work.

The certification authority has the right to interrupt the certificate service for modifications or maintenance. Modifications to or maintenance of the revocation list will be announced in advance.

The certification authority is not liable for errors in the online service or applications that are intended for end users and based on a certificate or any expenses arising from them.

The responsibility of a certificate holder ends when he or she, or a representative of the certificate holder's organisation, have reported to the certification authority the necessary data for revoking the certificate and when they have received a revocation notice from the person receiving the call. In order to terminate the liability, the revocation request must be made immediately upon noticing the reason for making the request.

7. Requirements applicable to the operation of the certification authority

The certification authority shall take management actions that meet the following requirements.

They include the offer of registration services, creation of certificates, distribution of certificates, revocation of certificates and communication about certificate revocation (see section 4.2). If the requirement is related to the certification authority's specific area of service, it is given under the corresponding heading. If no area of service is itemised below or if "certification authority in general" is mentioned, the requirement applies to the certification authority's general operations.

The purpose of these procedural requirements is not to restrict the certification authority's possibility of charging for the services.

The requirements presented here apply to the security objectives and the administrative means used to attain them, for which detailed requirements are presented if deemed necessary for meeting the objectives.

8. Certification practice statement

The certification authority prepares a certificate practice statement and other procedural instructions that complement the certificate policy. The certification authority ensures that certificate policies, certification practice statements and PKI disclosure statements are publicly available at https://dvv.fi/en/certificate-policy.

The rights and obligations of a service certificate applicant are specified in the application document and general terms and conditions, which comprise the contract concluded with the certificate applicant.

The application document and the terms and conditions of use clearly state that the applicant for a service certificate, with his or her signature, confirms the correctness of the information provided and approves of the creation of the service certificate and its publication in the public directory. At the same time, the applicant accepts the rules and terms pertaining to the use of the service certificate and the obligation to report any misuse or disclosure of a private key.

The certification authority specifies and approves the certification practice documents.

The certification authority ensures that its certification activity and certification practice conform to this certificate policy.

The certification authority's operation is audited at least once a year. In the audit, the certificate policy and the certification practice statement are compared to the certification authority's activities across the board. If non-conformities are found, the certification authority will take action to rectify them without delay.

The algorithms and other technical details used in certification and certificates are described in section 7.2.

9. Life cycle management of keys used in a public key infrastructure

5.1.1 Creation of certification authority's keys

The certification authority generates its private signature keys and corresponding public keys. The certification authority's private keys are stored in hardware security

modules administered by the certification authority, which meet the requirements of the necessary security standard.

It is possible that Digital and Population Data Services Agency issues a certificate for it´s own purposes. In that case it follows the same requirements than issuing certificates for other organisations.

The certification authority sees to it that the certification authority's private keys are protected against disclosure and unauthorised use. A backup copy is made of the certification authority's private keys in a manner that is suitable for ensuring critical information security.

The keys are stored in hardware security modules administered by the certification authority. The modules meet FIPS 140-1 Level 3 requirements.

The certification authority's private key, which is used to sign service certificates, and the corresponding public key are 4096-bit RSA keys.

The lengths of the private and public key of the service certificate are up to the certificate applicant. The key length of a service certificate issued by the Digital and Population Data Services Agency is 4,096 bits at minimum.

The certification authority creates a new key pair and CA certificate no later than five years and three months before the expiry of the previous CA certificate. The CA certificate is submitted to a public directory as described in section 7.3.5.

The generation of the private key requires the simultaneous presence of, or activation of a function by, at least two persons.

5.1.2 Storage, backup and recovery of the certification authority's key

The certification authority's private keys are protected against disclosure and unauthorised use.

The keys are stored in hardware security modules administered by the certification authority. The modules meet FIPS 140-1 Level 3 requirements.

A backup copy of the certification authority's private key exists.

The security features and storage of the backup copy are compliant with the security requirements pertaining to the original certification authority private key in all circumstances.

The private keys and their backups are stored with strong encryption in devices that meet the requirements of critical information security.

5.1.3 Distribution of the certification authority's public key

The CA certificate containing the certification authority's public key can be retrieved from the public directory or a service provided by the certification authority. The certification authority publishes its public key in a publicly accessible directory at ldap://ldap.fineid.fi and its website at https://dvv.fi/en/.

5.1.4 Backup key system

The signatory’s private signature keys are not stored in a way that enables decryption and backup copying, which would allow authorised parties in certain situations to undo the encryption by utilising information from one or more parties.

5.1.5 Use of the certification authority’s key

The field that determines the intended use in the certificate’s data content specifies the intended use of the key pertaining to the certificates.

The CA certificate is only used to sign service certificates and revocation lists associated with them. For a technical description, see the FINEID S 2 specification.

Once the CA certificate expires, the certification authority's private keys in the security module are destroyed and will not be reused.

The certification authority's private keys are encrypted and stored in security modules.

The certification authority's private keys are activated by authorised personnel using security module management cards. The use of the certification authority's private keys is prevented by authorised personnel using management cards or by disconnecting power from the security module where the certification authority's private keys are stored.

The certification authority has the right to transfer its private keys to another security module if the original HSM is replaced or decommissioned for service.

The certification authority's private keys are destroyed after expiry. The certification authority's private keys can only be destroyed by the certification authority. If the certification authority's operations are terminated, its private keys and their copies are destroyed.

The certification authority creates a certificate holder’s key pair where necessary. The certificate and the associated key pair and password are then delivered to the certificate holder using a method that prevents unauthorised access.

The secure key pair creation and storage process prevents the exposure of the keys beyond the key creation system.

10. Life cycle management of certificates used in a public key system

5.1.6 Signatory registration

The certification authority must ensure that the signatories are appropriately identified and authenticated and that the signatory’s certificate requests are complete, true and appropriately authorised.

The official name and other data submitted by the applicant and verified by the registration authority are used when naming the service certificate holder.

The set of attributes that forms the name record in the certificate is unique and identifies the certificate holder in question. All service certificate holder organisations must operate under their own names.

The certificate holder’s private keys for a server or a system signature certificate are created on the certificate holder’s or their technical supplier’s server. In the case of an e-mail service certificate, the certification authority creates both the key pair and the certificate and delivers them to the certificate holder.

Authentication of the certificate holder's organisation

The rights and obligations of a service certificate applicant are specified in the application document and general terms and conditions, which comprise the contract concluded with the certificate applicant.

The application document and terms and conditions of use clearly state that the applicant for a service certificate, with his or her signature, confirms the correctness of the information provided and approves of the creation of the service certificate and its potential publication in the public directory. At the same time, the applicant accepts the rules and terms pertaining to the use of the service certificate and the obligation to report any misuse or disclosure of a private key.

An agreement has been concluded between the certification authority and the registration authority as well as other vendors that provide parts of the certificate services, indisputably specifying the rights, liabilities and obligations of both parties.

A service certificate applicant is responsible for ensuring that all information submitted by them to the certification authority or registration authority essential for the certificate is correct. The service certificate holder must only use the service certificate for its intended purposes.

When a certification authority issues a service certificate, it also approves the application for a certificate.

The certificate holder must immediately report the service certificate to the revocation list if they suspect that their service certificate may have been used in breach of the terms and conditions.

Service certificate applications should be submitted on the form that can be downloaded and printed at https://dvv.fi/en/.

Before issuing the certificate, the certification authority will check the applicant's information in such sources as the Virre register in the online service of the Finnish Patent and Registration Office. In this connection, the Digital and Population Data Services Agency will verify the domain name by means of an e-mail message. A proxy should be submitted together with the application if the certificate holder (IT contact person or similar) is acting on behalf of a company or an organisation. The information of central or local government authorities and parishes will not be checked in the Virre register. The Digital and Population Data Services Agency must have access to any domain names ending with .fi and information on their administration when processing the application. Other domain names will be checked using any available

online services or other reliable methods. The Digital and Population Data Services Agency only issues server certificates for IP addresses or domains used for public administration purposes.

If the applicant is a private individual, the applicant should submit the service certificate application to the certification authority in person. The applicant's identify is then verified using an identity document issued by the police, which are an identity card, a passport and a driving licences issued after 1 October 1990.

Other acceptable identity documents are: a valid passport or identity card issued by an official government agency of an EEA member state, Switzerland or San Marino, a valid driving licence issued by an official government agency of an EEA member state after 1 October 1990, or a valid passport issued by an official government agency of another state.

A service certificate will be issued for no more than 12 months. The same procedure should be used for renewing a certificate as when submitting the original application. The price of the certificate is based on the annual fee indicated in the Digital and Population Data Services Agency's service price list.

The certification authority issues a service certificate when accepting the application for a certificate.

When issuing a certificate, the certification authority is responsible for ensuring that the certificate's data content is correct at the time of certificate delivery.

When processing certificate requests, the public key is tested for known weaknesses using a software tool.

Once issued, the service certificate is delivered to the customer as agreed.

The CA checks CAA records while processing certificate registrations, and recognizes the 'dvv.fi' and 'fineid.fi' issuer domain name.

5.1.7 Renewing a certificate, changing the key pair and updating a certificate

A certificate should also be renewed if the certificate holder's details change (insofar as it affects the data content of the certificate). In this case, the certificate holder must contact the certification authority and apply for a new service certificate.

If the use of the certificate holder's private key is blocked, the certificate linked to this key must be renewed.

Certificate renewal may only be applied for by a representative of the certificate holder organisation or a party authorised by it.

When renewing certificates, the same procedures should be followed as when applying for a certificate for the first time.

The data contents of a certificate cannot be altered after the certificate has been created. When the information that affects the certificate's data content changes, the holder should apply for a new service certificate.

The same procedures are followed to renew a service certificate as when applying for it for the first time. When a certificate holder renews their private key, re-registration, a new certificate application and a new service certificate are always required.

5.1.8 Creation of certificates

For the data content of a certificate, see the FINEID S2 specification at https://dvv.fi/en/.

The certification authority's private keys are stored in security modules administrated by the certification authority which meet FIPS 140-1 or 140-2 level 3 requirements. The certification authority’s private keys are protected against disclosure and unauthorised use.

The CA certificate is signed by the root certification authority and placed in a public directory.

Naming policies:

CN (Common name) = VRK Gov. Root CA – G2

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

The Digital and Population Data Services Agency's certification authority for server certificates is:

CN (Common name) = VRK CA for Social Welfare and Healthcare Service Providers - G2

OU (Organizational unit) = Sosiaali- ja terveydenhuollon palveluvarmenteet

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Certification holder naming practice for server certificates (mandatory fields):

SERIALNUMBER (Serial Number) = Serial number

CN (Common Name) = Name of service (”www.fineid.fi”)

O (Organization) = Organisation name (for example, Yritys Oyj)

C (Country) = FI

Optional fields:

E (Email address) = E-mail address (”webmaster@yritys.fi”)

OU (Organizational Unit) = Organisation unit (”Information Management”)

STREET (Street Address) = Street Address (“ Lintulahdenkuja 4”)

PC (PostalCode) = Postal code (“00530”)

L (Locality name) = City or municipality (”Helsinki”)

S (State or province name) = State (”Suomi”)

DNS (DNS Name) = DNS Name (”www.yritys.fi”)

Data pertaining to the holder of a CA certificate unambiguously identifies the certificate holder organisation.

The certification authority's private keys are activated by authorised personnel using HSM management cards.

The certificate holder's private keys are protected against disclosure and unauthorised use in the holder’s information system. Private keys stored in the chip can only be accessed by internal commands performed in the information system.

In order for a command related to the private keys to be executed, the key must be activated using the correct password.

Archived data are stored in facilities with high-level security and access control.

The CA certificate containing the certification authority's public key can be retrieved from the public directory or a service provided by the certification authority.

5.1.9 Distribution of terms of use

The certification authority must ensure that the terms and conditions of use are made available to the customers and the parties relying on certificates.

The CA certificate containing the certification authority's public key can be retrieved from the public directory or a service provided by the certification authority.

Changes concerning the certificate policy other than those specified in section 8 will be published by the certification authority on its website (https://dvv.fi/en/certificate-policy) at least 30 days before the change takes effect.

The certification authority publishes all service certificates and revocation lists in a non-chargeable, openly available public directory. The certification authority publishes the certificate policy, the certification practice statements, the PKI disclosure

statement and other public documents pertaining to the production of certificate services on its website https://dvv.fi/en/certificate-policy.

Availability of data

Directory and revocation list data are publicly available. The FINEID specifications published by the certification authority are available on the certification authority's website at https://dvv.fi/en/. In addition, the certificate policies and certification practice statements are available on the certification authority's website at https://dvv.fi/en/certificate-policy.

Repositories

The information published by the certification authority is available on the certification authority's website at https://dvv.fi/en/. Confidential data used in the certificate system are stored in the certification authority's own confidential repository. The certification authority's data are archived according to the valid archiving rules. Special attention is paid to the handling of personal data, and the Digital and Population Data Services Agency has published a specific set of procedures for the provision of certificate services in accordance with the Personal Data Act. The certification authority has also prepared a file description referred to in the Personal Data Act for the processing of personal data in each area of the certificate system, and these descriptions have been published on the certification authority's website at https://dvv.fi/en/.

5.1.10 Distribution of certificates

Each certificate is published in the public directory immediately upon its creation, and it remains in this directory for as long as it remains valid. The certification authority publishes a revocation list that is valid for two days after its publication. This revocation list is updated once an hour.

Directory and revocation list data are publicly available at ldap://ldap.fineid.fi.

5.1.11 Revoking a certificate and placing it in a suspended state

Revocation and suspension of a certificate

The certification authority maintains a certificate revocation service. Details of revoked certificates are published on a certificate revocation list, which is signed by the certification authority and published in a public directory. Certificates cannot be temporarily suspended.

The certification authority does not notify certificate holders if their certificates are revoked.

Prerequisites for revoking a certificate

A certificate can be revoked:

- upon the certificate holder's request

- when information that affects the data content of the certificate holder’s certificate has changed
- a private key linked to the certificate has been lost or compromised
- the certificate holder organisation has ceased to operate.

No attempt must be made to use the certificate after the revocation request has been made.

Who can request revocation of a certificate

A certificate revocation request can be made by:

- a representative of the service certificate holder organisation;
- the service certificate holder
- the certification authority, if the conditions specified in section 6.2 are met.

Certificate revocation process

The certificate holder contacts the certification authority to make a revocation request. The request can be made:

1. by telephone
2. n person by visiting the registration point, or
3. by contacting the certification authority in writing.

The certification authority's official duties include the revocation of certificates:

- as a certificate holder organisation ceases to operate.

When revoking the certificate, the following information is recorded:

- identifying data of the service certificate
- personal data of the person making the revocation request
- organisation of the person making the revocation request
- the method used to identify the person making the revocation request
- time and date of the revocation request
- reason for the revocation request
- personal data of the person receiving the revocation request

- other additional information provided by the certificate holder
- the time and date when the key pair was compromised, the date on which the certificate holder organisation ceased to operate or similar
- details of the person executing the revocation
- the date of revocation.

The certification authority will not send the certificate holder a separate confirmation of having revoked the certificate. The data related to the revocation will be kept on file for 10 years.

Certificate holder's duty to request revocation

The certificate holder must request revocation of his or her certificate immediately by contacting the certification authority if the conditions for revoking the certificate set out in section 6.2 are met.

Revocation request processing time

The certification authority processes certificate revocation requests immediately.

The relying party's duty to verify the validity of a certificate

The relying party is responsible for verifying that the certificate is valid and that it has not been revoked before accepting the certificate.

The relying party is responsible for checking the valid revocation list. The certificate should not be trusted before the relying party has checked the revocation list.

Publishing frequency of the revocation list

An updated revocation list is published every hour.

It indicates the scheduled publication time of the next revocation list. The next list may be published before the scheduled time.

Maximum validity period of the revocation list

Each updated revocation list is valid for no more than 48 hours. Each list specifies the end time of its validity.

The holder of a service certificate may have the certificate revoked before the expiry of its validity period.

Revocation request procedure

The service certificate holder or an authorised representative of the certificate holder organisation must notify the Digital and Population Data Services Agency’s Certificate Services if they know or suspect that the certificate holder’s private key has been compromised. The notification should be submitted by telephone during office hours to +358 (0)9 2291 6748, by fax to +358 (0)9 2291 6795 or by an e-mail message signed using a qualified certificate issued by the Digital and Population Data Services

Agency to kirjaamo@dvv.fi. The notification should contain the following information: the name and organisation of the person making the notification, and the serial number of the service certificate to be revoked. The certification authority revokes the certificate in question once it has received the notification. When the certificate holder has submitted a revocation request to the certification authority and the revocation has been confirmed (during the telephone call, by fax or by e-mail depending on how the notification was submitted), the certificate holder no longer is responsible for the use of the certificate.

11. The certification authority’s management and operating procedures

The Digital and Population Data Services Agency maintains a classification of importance for certificate service objects and systems, their backups, priorities and minimum maintenance levels.

5.1.12 Security management

The Digital and Population Data Services Agency's information security is managed according to the Digital and Population Data Services Agency’s information security policy and standard ISO 27001.

5.1.13 Repository classification and management

The Digital and Population Data Services Agency is an agency subordinate to the Ministry of Finance. The certificate services it provides are covered by a financial administration system and supervision as laid down in specific provisions. The financial management of the Digital and Population Data Services Agency is based on the acts and decrees that govern central government finances and regulations issued by the Ministry of Finance and the State Treasury. The National Audit Office is responsible for the DPDSA’s financial oversight. In addition, its performance is reviewed from the points of view of effectiveness, economy and productivity.

In compliance with the general Terms and Conditions of Public IT Procurement (JIT 2007), the Digital and Population Data Services Agency ensures that it has adequate financial resources for proper arrangement of certificate operations and for covering possible liabilities.

5.1.14 Staff and information security

The Digital and Population Data Services Agency serves as a certification authority responsible for certification activities. The technical vendors have been selected through competition and work at the responsibility and on behalf of the Digital and Population Data Services Agency.

The Digital and Population Data Services Agency pays particular attention to the reliability of both its own staff and the technical vendors and registration authorities and to their skills needed for the execution of the tasks.

Background checks

The Digital and Population Data Services Agency requests for a basic security clearance for its staff and technical vendors who work with the certificate environment.

Procedure adhered to in the security clearance

The staff's work experience is scrutinised at the time of recruitment. A basic security clearance is requested for each person based on the information he or she has provided on a standard form.

All relevant personnel of the certification authority, certificate service and directory service providers and those performing key tasks in the revocation service must:

- complete a form which is submitted to the Finnish Security Intelligence Service for basic background check purposes
- refrain from duties which are in conflict with their obligations and responsibilities
- not be persons known to have been released from a previous duty on the grounds of negligence of duty or misconduct
- be appropriately qualified for the duties they are taking on.

Training requirements

The Digital and Population Data Services Agency's staff must be trained so that duties can be carried out in the optimal way. The Digital and Population Data Services Agency has a training plan, the implementation of which is the responsibility of the Digital and Population Data Services Agency's administration unit.

Maintenance of expertise and skills

Staff training is planned and maintained in such a way that the expertise related to the management of the task is always at the best possible level required by the task.

Requirements for task rotation

When planning for task rotation in the certification authority's tasks, the tasks must be organised in such a way that the employee can perform his or her new duties in an optimal way. Keeping up good information administration practices and maintaining a sufficient level of task-specific skills are taken into consideration in the planning of the task rotation.

Task rotation also adheres to the Digital and Population Data Services Agency's information security policy and information security plan as well as the Digital and Population Data Services Agency's other general instructions.

Measures resulting from deviations

The Digital and Population Data Services Agency's staff are subject to liability for acts in office and work following the internal instructions of the Digital and Population Data Services Agency. Provisions on the position of a public official are laid down in the state officials act (valtion virkamieslaki, 750/1994).

Staff representing the organisation

When recruiting staff, it must be ensured that the staff's skills correspond to the requirements of the tasks and that no circumstances revealed in the background check put an employee's interests at odds with the production of certificate services.

Documents given to the staff

The staff always has access to the Digital and Population Data Services Agency's quality and security documents.

5.1.15 Physical security and security of the environment

The Digital and Population Data Services Agency uses technical vendors for carrying out the information technology tasks of the certificate service. The DPDSA is responsible, as the certification authority, for the safety and operation of certificate production in an appropriate way in all of its areas.

Location and building properties

The certification authority's systems are located in high-security data centres and meet the guidelines and orders imposed on data centres regarding security.

Facility safety has been implemented in such a way that unauthorised access to the facilities is prevented.

Physical access to facility

Facilities where production duties for the certificate system are carried out have controlled physical access. The access control system detects authorised and unauthorised entry. Access to data centre facilities requires the identification of the person, whereby the person is identified, his or her access right is verified and the transactions are registered. Data centre facilities are guarded at all times of the day.

Auxiliary arrangements

The hardware solutions have been implemented according to good information administration practice in such a way that in the event of system failure, a backup system can be used without compromising the confidentiality, integrity or availability of the data contained in the system.

The supply and maintenance of spare parts for important devices has been ensured.

5.1.16 Operations management

The Digital and Population Data Services Agency uses technical vendors for the registration and information technology duties of certificate production. The Digital and Population Data Services Agency serves as a certification authority responsible for certification activities.

The certification authority's tasks are comprised of the following areas of responsibility:

- Information security
- Registration
- System administrator
- System user
- System supervisor

The certification authority and the technical supplier have concluded a supply agreement which contains detailed descriptions of the supplier's duties, methods and responsibilities and the information security provisions.

5.1.17 Management of access to systems

The creation, activation, backup and recovery of the certification authority’s private keys require the presence of two persons with administrator privileges.

At least two persons authorised to carry out maintenance on the system are present when the certification authority’s private key’s hardware security module is initialised.

The use of the system requires the presence of at least one person authorised to do so.

The registration and identification of a service certificate requires the presence of one person.

5.1.18 Commissioning and maintenance of systems to be trusted

Registration authority of the server certificate: The registration authority is the Digital and Population Data Services Agency’s Certificate Services.

The certificate system administrator: Identified on the basis of a personal system management card. System administrators include the system specialists of the certificate system supplier and authorised personnel of DPDSA.

Certificate system user: Identified on the basis of a personal system access card. The certificate system's users include data centre operators, technical certificate request initiators, and the revocation service.

5.1.19 Business continuity management and processing of anomalies

The Digital and Population Data Services Agency has a continuity and preparedness plan that enables the continuity of the certification operations.

The certification authority’s private key has become disclosed or the certificate has been revoked

In each certification practice statement, the root certification authority states the measures that the root certification authority, the CA certificate holders, parties relying on the CA certificate, registration authorities and the root certification authority’s

staff must take if the root certification authority's private key has become disclosed or otherwise unusable.

In such cases, the root certification authority will either suspend its service as described in section 7.4.9 or carry out the following measures:

a) The root certification authority notifies all CA certificate holders, relying parties, and customers with whom the certification authority has agreements in place or who are otherwise, on the grounds of a contractual relationship or government activities, in a relationship with the root certification authority that entitles them to be notified by the root certification authority.

b) The root certification authority creates a new key as described in section 7.3.3.

c) All CA certificates and end user certificates that are valid and have been issued using the exposed key must be revoked on one or several revocation lists whose validity period does not expire until the validity of the last revoked CA certificate has expired.

Compromised security because of a natural disaster or other catastrophe

The Digital and Population Data Services Agency's security policy takes into account the measures necessitated by the compromising of external security. The Digital and Population Data Services Agency is ISO 27001 certified with respect to information security, which also sets requirements for the Digital and Population Data Services Agency's operations after the occurrence of a catastrophe.

5.1.20 End of the certification authority's operation

The termination of the certification authority is considered to be a situation where all services related to the issuing of CA certificates are permanently terminated. The termination of the certification authority does not refer to a situation where the certification service is transferred from one organisation to another.

The certification authority communicates about the termination of the certificate services as soon as possible, however at least one month before the time of termination.

Before the termination of the certification authority, at least the following measures shall be taken:

a) All service certificates that are valid and have been granted are closed on one or several revocation lists whose validity period does not expire until the validity of the last revoked certificate has expired.

b) The certification authority revokes all authorisations of its contracting partners to carry out tasks pertaining to certificate issuing process on behalf of the certification authority.

c) The certification authority ensures that access to the certification authority's archives will be maintained also after the termination of the certification authority.

5.1.21 Applicable legislation

The Digital and Population Data Services Agency complies with the valid Finnish legislation in its certificate service activities.

Provisions on the certificates issued by the Digital and Population Data Services Agency are contained in the Act on the Population Information System and the Certificate Services of the Digital and Population Data Service Agency (661/2009).

The Digital and Population Data Services Agency's liability related to the provision of certificate services is determined under the valid cooperation agreements and pursuant to the provisions in the Tort Liability Act (412/1974). In addition, the requirements laid down in the Act on Strong Electronic Identification and Trust Services (617/2009) apply to the Digital and Population Data Services Agency.

5.1.22 Retention of information pertaining to certificates

The information published by the certification authority is available on the certification authority's website. Confidential data used in the certificate system are stored in the certification authority's own confidential repository. The certification authority's data are archived according to the valid archiving rules. Special attention is paid to the handling of personal data, and the Digital and Population Data Services Agency has published a specific set of procedures for the provision of certificate services in accordance with the Personal Data Act. The certification authority has also prepared a description of file for each component of the certificate system compliant with the Personal Data Act with respect to the processing of personal data.

The provisions of the archive act (arkistolaki, 831/1994) are applied as the general act on archiving. The right to obtain information is determined according to the Act on the Openness of Government Activities (621/1999). With respect to the archiving of certificates, the provisions pertaining to archiving in electronic services legislation are also applied. Certificate register data will be kept on file for at least 10 years after certificate expiry. The certification authority archives the following information:

a) The application form signed by the applicant, and the acknowledgement of receipt of the service certificate and the associated terms and conditions.

b) Issued server certificates, their data contents and additional details related to their life cycle management starting from the time of expiry or revocation of the certificate.

c) Events related to the creation or renewal of the certification authority's private key

d) Server certificate revocation requests

d) Revocation lists saved to the public directory and other information related to server certificate revocation

f) Current and previous versions of the certificate policy and the corresponding certification practice statements

g) User actions by the administrators and users of the certificate system who are registered users of the certificate system are recorded in log files

h) Audit reports and records, including information security audits and system audits.

The archive data are stored in accordance with regulations pertaining to the qualified certification authority in question.

Protection of archives

The certification authority stores the archived documents related to server certificate application, the applicant's identification and server certificate delivery in appropriate facilities.

Archived data are stored on high-security premises with access control.

Backup methods for archived data

Backup copies are stored in a place physically separate from the original data.

Acquisition and backup methods for archived data

If a certification authority’s service is interrupted or terminated, the authority shall notify all of its customers that the archive will continue to be available. All archive queries should be sent to the certification authority or some other party designated by the authority before it terminates its service.

The certification authority ensures the availability and readability of the archives, also in the event that the certification authority’s operations are interrupted or terminated.

Archived data will be made available as deemed appropriate from the point of view of the server certificate holder or the relying party.

12. Organisation requirements

The Digital and Population Data Services Agency is a public authority which administers a personal data file and, under the Act on the Population Information System and the Certificate Services of the Digital and Population Data Service Agency (661/2009), is responsible for providing certified electronic services in addition to its other tasks.

The Digital and Population Data Services Agency issues certificates on application. The rights and responsibilities of a certificate applicant are specified in the Digital and Population Data Services Agency’s certificate application document and the general terms and conditions of use, which comprise a contract concluded with the certificate applicant.

An agreement has been concluded between the Digital and Population Data Services Agency and the Registration Authority as well as other vendors that provide parts of the certificate services, indisputably specifying the rights, liabilities and obligations of both parties.

The certificate services produced by the Digital and Population Data Services Agency are covered by a financial administration system and supervision as has separately been set forth. The Digital and Population Data Services Agency is a government agency under the Ministry of Finance. The financial management of the Digital and Population Data Services Agency is based on the acts and decrees that govern central government finances and regulations issued by the Ministry of Finance and the State Treasury. The National Audit Office is responsible for the DPDSA's financial oversight. In addition, its performance is reviewed from the points of view of effectiveness, economy and productivity.

The Digital and Population Data Services Agency complies with the valid Finnish legislation in its certificate service activities. The Digital and Population Data Services Agency performs its duties carefully, reliably and appropriately. The Digital and Population Data Services Agency keeps publicly available information regarding its certificates and certificate activities, based on which the operation and reliability of the certification authority can be assessed.

The Digital and Population Data Services Agency pays particular attention to the reliability of both its own staff and the technical vendors and registration authorities and to their skills needed for the execution of the tasks. The Digital and Population Data Services Agency has the necessary technical ability and financial resources for appropriately arranging the certificate activities and for covering potential liability for damages. The Digital and Population Data Services Agency's staff are subject to liability for acts in office and work following the internal instructions of the Digital and Population Data Services Agency. Provisions on the position of a public official are laid down in the state officials act (valtion virkamieslaki, 750/1994).

Any disputes shall be settled according to Finnish law. Valid legislation is adhered to in settling appeals and disputes, in administrative supervision and implementation of law.

13. . Framework for the specification of other certificate policy documents

This section specifies the general framework for other certificate policies of certification authorities issuing certificates. A certification authority can confirm their compliance with this general specification framework as set out in section 8.3. In general, a precondition for compliance is complying with the requirements in sections 6 and 7, excluding the requirements that apply to certification authorities that only issue certificates to the general public.

14. Specification document management

Modifications to specifications

The certification authority may change the specifications because of legislative, operative or technical requirements. Changes to the specifications must be recorded in the certificate policy and certification practice statement documents as described below.

Publication and communication

The certification authority publishes a certificate policy and a certification practice statement, available at the website https://dvv.fi/en/certificate-policy.

The certification authority's public specifications pertaining to the production of certificates can be obtained from the same websites.

The agreements concluded with information technology vendors on the delivery of certificates and production system descriptions and product-related specifications are confidential.

Modification and approval procedure of the certification practice statement

The Digital and Population Data Services Agency approves the certificate policy and certification practice statement pertaining to service certificates. These documents may be modified according to the Digital and Population Data Services Agency's internal change policy.

The Digital and Population Data Services Agency will communicate the changes to Traficom and on its own website well in advance of their entry into force.

The Digital and Population Data Services Agency maintains version management of the documents and archives all certificate policy and certification practice statement documents. Typographic corrections and changes of contact details may be made with immediate effect.

1. All items of the certificate policy and certification practice statement can be amended by communicating the main upcoming changes 30 days before their entry into force.

2. Items that Digital and Population Data Services Agency does not deem to have significant effect on certificate holders and trusting parties may be amended with communication 14 days in advance.

15. Additional requirements

In the context of fulfilling the requirements specified in section 7.3.4, the customers and the relying parties shall be informed of how each current policy adds to, or restricts further, the certificate policy requirements as they are specified in this document.

16. Compliance

The certification authority may only state it works in compliance with this certification practice statement

a) if the certification authority confirms that they comply with an identified certificate policy and, on request, makes proof of compliance available for the customer and relying parties. The proof may, for example, include an auditor’s report that confirms the certification authority's compliance with the requirements of an identified certificate policy. While this may be an auditor internal to the certification authority’s organisation, the auditor must not have a hierarchical relationship with the certification authority implementing the operations.

b) if a qualified and independent party has recently assessed the present state of the certification authority's adherence to the requirements of a uniquely identified certificate policy. Upon request, the assessment results must be made available to the customers and relying parties.