DIGITAL AND POPULATION DATA SERVICES AGENCY

CERTIFICATION PRACTICE STATEMENT ROOT CERTIFICATE

For the Digital and Population Data Services Agency's root certificate
OID: 1.2.246.517.1.10.201

6.5.2021

Tel. **+358 295 536 000** (exchange) | Contact Information, see **www.dvv.fi/en**

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 v 1.0., published on 14 December 2017	14/12/2017
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	6.5.2021

Table of contents

Definitions and abbreviations

Definitions

Activation data: Confidential data that, in addition to RSA keys, is needed to use cryptographic modules (including basic PINs and signature PINs).

Key pair: A pair of interconnected keys, one public and one private, which are used in public key methods. The keys' purpose is defined in the certificate (see certificate holder's signature certificate and authentication and encryption certificate).

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.

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: Information security infrastructure in which security services are provided using the public key method.

Public key method: An information security service, such as electronic identification, provided by using a public and a private key, certificates and asymmetric encryption.

Root certification authority: An organisation that issues CA certificates and formulates a certificate policy describing its activities as well as a certification practice. In this certification practice, the Digital and Population Data Services Agency serves as the root certification authority.

Citizen certificate: A certificate for secure use of e-services issued by the Digital and Population Data Services Agency to a natural person governed by the Act on the Population Information System and the Certificate Services of the Population Register Centre.

Relying party: The party that relies on the certificate data and uses the certificate to access different security services, including authentication, confidentiality and signature certification, when the certification authority's signature associated with the certificate is a match.

OID: Object Identifier, a unique identifier. The unique identifier OID of this certification practice is part of the data content of each CA certificate issued by the root certification authority.

PDS: PKI Disclosure Statement, a certificate description. A document that provides a general description of the different areas of the certification authority's activities.

RSA algorithm: An asymmetric public key algorithm.

Registration authority: The registration authority identifies the certificate applicant in accordance with the certificate policy and certification practice statement by commission of the certification authority.

Revocation list: A list of certificates that have been revoked before their expiry. A certificate put on the revocation list cannot be re-activated. (Authority Revocation List, ARL).

Certificate: A digital certificate that associates the signature authentication data with the signatory and authenticates the signatory.

Certificate system: An IT system used to create certificates and sign revocation lists.

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

Certificate Policy (CP): A document describing how the root certification authority issues CA certificates. Additionally, the document describes such aspects as the parties' responsibilities. The certificate policy must be publicly accessible.

Certificate register: A register conformant to the Act on Strong Electronic Identification and Trust Services that a Certification Authority providing certificates to the public must maintain for a set period of time.

Certification practice (CPS): A more detailed description of how the root certification authority implements its certificate policy.

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.

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.

CA certificate: A certificate issued by the root certification authority (CA). Contains the public key that corresponds to the private key issued by the certification authority used to authenticate the certification authority's electronic signature.

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

Certificate holder: An organisation whose public key has been certified with the root certification authority's private key and whose identifying data are contained in the CA certificate.

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.

Acronyms

ARL	Authority Revocation List
CA	Certification Authority

CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FINEID	Finnish Electronic Identification
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
eID	Electronic identification of a person
HTTP	Hypertext Transfer Protocol
ISO 27001	ISO/IEC 27001
LDAP	Lightweight Directory Access Control
OCSP	Online Certificate Status Protocol, an online service for checking the status of a certificate
OID	Object Identifier
PDS	PKI Disclosure Statement, certificate description
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman
SIM	Subscriber Identity Module
DPDSA	Digital and Population Data Services Agency

1 Introduction

The certification practice statement is a document drawn up by the 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.

This certificate practice statement is applied to the root certification authority's certificate (VRK Gov. Root CA – G2) of the Digital and Population Data Services Agency.

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.

1.1 General points

The Digital and Population Data Services Agency's certificate services are based on the public key infrastructure (PKI). The DPDSA's certificate infrastructure consists of a certificate system, a supplier of certificate data contained in the certificate cards, a revocation list, an advisory service and a directory service. The DPDSA's activities as a certification authority include the provision of certification, directory and revocation services, registration, and the creation and individualisation of a card that contains the certificate. The DPDSA is responsible for the functioning of the certificate system as a whole, including any registration authorities and technical suppliers it may use.

DPDSA draws up a separate certificate policy for each type of certificate issued by it, and a separate certification practice statement for each technical platform. The certificate policy contains a general description of the practices, terms and conditions, responsibility allocation and other matters related to certificate usage for each type of certificate. The certification practice statement contains a detailed description of the applicable practices. Each document is identified by an OID. The documents are available online at www.fineid.fi.

The DPDSA's certificate activities are based on provisions on identification and trust services laid down in 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 (Regulation).

The Digital and Population Data Services Agency's trust services meet the requirements contained not only in the eIDAS Regulation but also in standard EN 319 401 for qualified trust service providers and standard EN 319 411-1 for qualified trust service providers issuing certificates.

The certificates issued by the Digital and Population Data Services Agency are signature certificates and means of strong electronic identification in accordance with the Act on Strong Electronic Identification and Trust Services (617/2009). The DPDSA also issues other personal and software certificates within the same reliable system of the certification authority.

The Digital and Population Data Services Agency's trust structure is hierarchic: the PCR has a single root certification authority that issues certificates to other certification authorities. A certification authority may be either the Digital and Population Data Services Agency or some other public or private organisation.

The Digital and Population Data Services Agency introduced a new certificate system on 14/12/2017. The Digital and Population Data Services Agency's trust model is hierarchic: the PCR has a single root certification authority that issues certificates to other certification authorities. A certification authority may be either the Digital and Population Data Services Agency or some other public or private organisation.

This document describes the practices that the root certification authority follows when issuing certificates to the certification authority granting Government citizen certificates. End user certificates are not issued by the root certification authority: these are issued by the certification authorities certified by the root certification authority, each of which have their own certificate policies and certification practices.

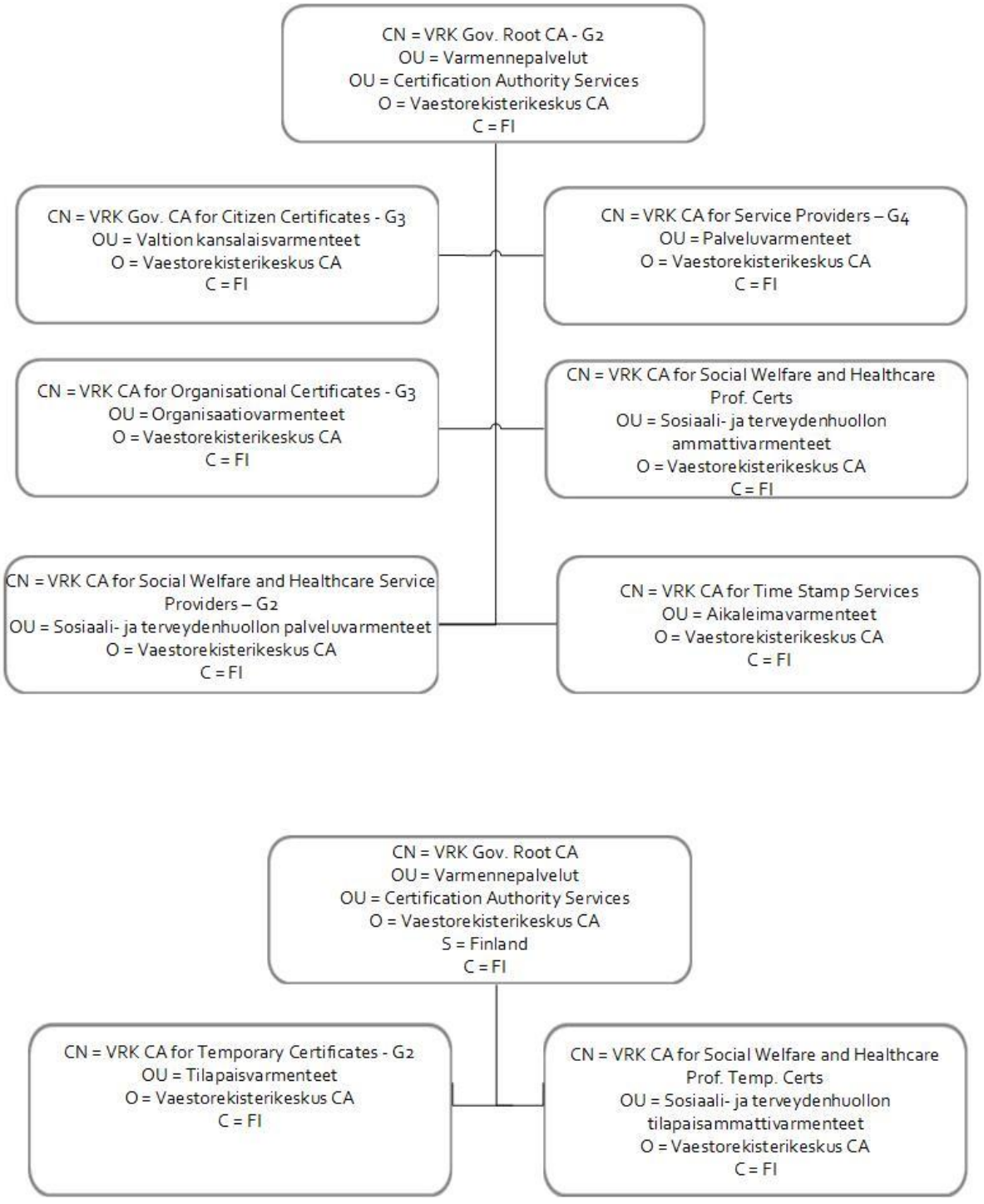

Figure 1: Certificate hierarchy

The CA certificate includes the CA's public key, name, the intended use and period of validity of the certificate as well as other information necessary for the use of the

certificate. The certificate data are signed electronically by the root certification authority's private key. CA certificates under this certificate practice statement are based on a public key infrastructure.

A private key that matches the public key in the CA certificate is used to sign electronically all citizen certificates that are issued and revocation lists that are published. The party relying on the CA certificate may verify its authenticity and integrity on the basis of the root certificate.

The Digital and Population Data Services Agency's Certificate Policy and Certification Practice documents have unique identifiers (OIDs).

The Digital and Population Data Services Agency draws up a separate certificate policy for the root certification authority as well as separate certificate policies for each type of CA certificate issued by the root certification authority. The Certificate Policy contains a general description of the practices, terms and conditions, responsibility allocation and other matters used by the certificate authority in its certification activities. The Certification Practice Statement contains a detailed description of the applicable practices.

1.2 Identifiers

The title of this certification practice statement is the Certification Practice Statement for the Digital and Population Data Services Agency's root certificate,

and it refers to the following certification practices of sub-certificates:

VRK Gov. CA for Citizen Certificates - G3, OID: 1.2.246.517.1.10.201.1

VRK CA for Organisational Certificates - G3, OID: 1.2.246.517.1.10.201.2

VRK CA for Temporary Certificates - G2, OID: 1.2.246.517.1.10.201.3

VRK CA for Service Providers - G4, OID: 1.2.246.517.1.10.201.4

VRK CA for Social Welfare and Healthcare Prof. Certs, OID: 1.2.246.517.1.10.201.5

VRK CA for Social Welfare and Healthcare Prof. Temp. Certs, OID: 1.2.246.517.1.10.201.6

VRK CA for Social Welfare and Healthcare Service Providers – G2, OID: 1.2.246.517.1.10.201.7

VRK CA for Time Stamp Services, OID: 1.2.246.517.1.10.201.8

This certification practice statement refers to the policy for the root certification authority of the Digital and Population Data Services Agency, OID 1.2.246.517.1.10.201.

The certificate policy and the certification practice statement are available at www.fineid.fi.

1.3 The root certification authority and the range of application of CA certificates

The root certification authority provides certificate services according to the terms and conditions specified in this certificate practice statement and guarantees their functioning in accordance with Chapter 2.2.1 on the responsibilities of the root certification authority. The root certification authority is responsible for the functioning of the certificate system as a whole, including any registration authorities and technical suppliers it may use. This certificate practice statement was registered by the Digital and Population Data Services Agency, which also serves as the CA certificate holder in accordance with this certificate practice statement.

The Digital and Population Data Services Agency is an authority that maintains a personal data file. Under the act on the Population Information System and the Certificate Services of the Population Register Centre, its task is to provide certificate services for e-service use. The DPDSA's Certificate Service is comprised of the following functions:

1.3.1 Root certification authority

The task of the root certification authority is to:

- issue CA certificates
- ensure the accuracy of the data content of the certificates issued by it
- provide certificate and directory services in accordance with its certificate policy and certification practice statement, and certification revocation services
- revoke CA certificates and publish CA certificate revocation lists (ARL).

1.3.2 Registration authority

The root certification authority is responsible for all tasks related to the registration of CA certificates.

- The registration authority identifies CA certificate applicants in accordance with the certification practice statement.

1.3.3 Directory service

The directory service is a public Internet service which can be used to retrieve all CA certificates issued by the root certification authority and the certification authority's latest revocation list. The directory service is available at ldap://ldap.fineid.fi.

1.3.4 CA certificate holder organisation

A CA certificate under this certificate practice statement has been issued to the Digital and Population Data Services Agency for granting citizen certificates.

The certificate holder organisation must comply with the root certification authority's Certificate Policy and Certification Practice Statement.

1.3.5 Trusting a CA certificate

The trusting party is a natural person or an organisation that trusts the CA certificate information and uses the root certification authority's certificate for verifying the authenticity and integrity of the CA certificate. The trusting party must verify that the CA certificate is valid and not on a revocation list.

1.3.6 Using a CA certificate

The purposes of using CA certificates referred to in this certification practice statement are: signing CA certificates and signing the certificate revocation list.

The Certificate Policy and Certification Practice Statement contain requirements related to the obligations of the root certification authority, a registration authority, a CA certificate holder and a relying party as well as matters related to legislation and dispute resolution.

1.4 Contact details

1.4.1 Organisation responsible for administering the certification practice statement

This certification practice statement was registered by the Digital and Population Data Services Agency. The centre is responsible for the administration and updating of this certification practice statement.

1.4.2 Contact person

Questions regarding this certification practice statement should be addressed to:

Digital and Population Data Services Agency

P.O. Box 123 (Lintulahdenkuja 2) Tel. +358 295 535 001

00531 Helsinki Fax. +358 9 876 4369

Business ID: 0245437-2 kirjaamo@dvv.fi

For inquiries concerning the certification policy, contact the registry office of the Digital and Population Data Services Agency, e-mail: kirjaamo@dvv.fi.

Digital and Population Data Services Agency (DPDSA) Certificate Services

P.O. Box 123

FI-00531 Helsinki

www.fineid.fi

2 General terms and conditions

This certification practice statement is effective as of 01/01/2020. The modification and publication procedure of the certification practice statement is described in Chapter 8 of this document.

2.1 Obligations

2.1.1 The obligations of the root certification authority

- The root certification authority shall act in compliance with current legislation.
- The root certification authority performs its duties carefully, reliably and appropriately.
- The root certification authority must have the necessary technical capabilities, financial resources and ability to cover its liability for damages.
- The root 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 root certification authority.
- The root certification authority draws up and maintains a Certificate Policy which describes at a general level the procedures for issuing, maintaining and managing CA certificates, the terms and conditions, the allocation of responsibilities, and other matters related to the use of CA certificates.
- The root certification authority draws up and maintains certification practice statements which describe how the root certification authority applies its certificate policy.
- The root certification authority complies with the certificate policy and certification practice statement requirements.
- The root certification authority makes the certificate policy and the certification practice statement publicly available.
- The root certification authority shall employ sufficient staff with the expertise, experience and competence required for producing certificate services.
- The root certification authority shall use reliable systems and products protected against unauthorised use.
- The root certification authority keeps publicly available information regarding its root certificates and certificate activities, based on which the operation and reliability of the root certification authority can be assessed.
- The root certification authority complies with the certificate policy and the certification practice statement in registration.

- The root registration authority identifies the CA certificate applicant reliably as described in the certification practice statement, ensuring that the applicant's information is carefully verified.
- The root registration authority shall see to the careful handling and confidentiality of the data.

2.1.2 The obligations concerning the CA certificate holder organisation

- The purposes of using CA certificates are: signing citizen certificates and signing the certificate revocation list. The certificate may only be used for the intended purpose.
- An organisation that holds a CA certificate is responsible for ensuring that the data provided in the certificate application is correct.
- The CA certificate holder organisation must store their private key in a secure environment and prevent its loss, disclosure to outsiders, modification or unauthorised use.
- The CA certificate holder organisation must notify the root certification authority immediately if it knows or suspects that the certificate authority's private key has been compromised. The root certification authority will then revoke the CA certificate in question and publish it on the revocation list (ARL).

2.1.3 Responsibilities of the party relying on a CA certificate

The root certification authority shall comply with the certificate policy and certification practice statement in issuing CA certificates.

A relying party may trust the certificate in good faith after verifying that the CA certificate is valid and not placed on the revocation list. The trusting party must check the validity of the CA certificates before accepting them. In order to reliably verify the validity of a CA certificate, the party relying on the certificate must comply with the following procedure for revocation list checks.

When a party relying on the CA 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 CA certificate of a certificate issued under this should be accepted if the validity period of the last retrieved revocation list has expired. All CA certificate and end user certificate approvals after the validity period are at the risk of the party trusting the CA certificate.

2.1.4 Obligations pertaining to the publishing of a CA certificate

CA certificates are published in a generally available public directory, and revoked CA certificates on a revocation list where a party trusting the certificate must check its validity.

2.2 Liabilities

2.2.1 Root certification authority's responsibilities

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

The Digital and Population Data Services Agency is responsible for ensuring that the CA certificates have been created in compliance with the Act on the Population Information System and the Certificate Services of the Population Register Centre and the Act on Strong Electronic Identification and Trust Services, and that it meets the certification authority's liability for damages. Digital and Population Data Services Agency is liable only for the data it has stored in the CA certificate.

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

The Digital and Population Data Services Agency ensures that the CA certificate has been released according to agreement to the organisation identified as required by the CA certificate.

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

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

2.2.2 Registration authority's responsibilities

The root certification authority serves as the CA certificate's registration authority. The CA certificate is applied from the root certification authority based on an application on the issue.

In all its activities, the root certification authority complies with the certification authority's responsibilities referred to in this section.

The root certification authority is liable for the damages pertaining to registration in accordance with this section.

2.2.3 CA certificate holder organisation's responsibilities

The CA certificate holder organisation is responsible for the use of the certificate, for the legal actions taken with it and the financial consequences of the legal actions.

The CA certificate holder organisation's responsibility for the certificate use ends when it has provided the root certification authority with the information on revoking the certificate in accordance with the agreement concerning the issue of the CA certificate. To end the responsibility of the CA certificate holder organisation, the

revocation request must be made immediately after giving the reason for making the request.

2.2.4 Responsibilities of a party relying on a CA certificate

A party relying on a CA certificate may not trust the correctness of a CA certificate in good faith if the validity of the certificate has not been checked against the revocation list. Accepting the CA certificate in the above cases releases the root certification authority from liability and responsibility.

A party trusting a CA certificate must verify that the certificate issued corresponds to its intended use

2.2.5 Limitations of liability

The root certification authority is not liable for damages and costs caused by the disclosure of a CA certificate holder organisation's private key unless the disclosure is the direct result of the root certification authority's actions.

The root certification authority is not liable for indirect or consequential damage caused to the CA certificate holder organisation. 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 organisation.

The root certification authority is not responsible for the operation of public telecommunication connections, such as the Internet, or for the inability to execute a legal transaction because of the non-functionality of a device or software used by the CA certificate holder organisation or for the use of a CA certificate in contradiction to its intended use.

The root certification authority has the right to develop the certificate service. The root certification authority is not liable to compensate the CA certificate holder organisation or a relying party for any expenses caused by the root certification authority's development work.

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

The root certification authority is not liable for errors in the online service or application based on the CA certificate or any expenses arising from them.

The CA certificate holder organisation's responsibility for certificate use ends when a representative of the organisation has provided the root certification authority with the information required to revoke the certificate and has also informed its most important partners and stakeholders related to certificate transactions of the matter. You should make the revocation request immediately after you have noticed the reason for making the request.

2.3 Financial liability

2.3.1 Root certification authority

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. Where applicable, the provisions of the Tort Liability Act (412/1974) also apply.

2.3.2 Other parties

A party trusting a CA certificate may trust the correctness of the CA certificate if they have verified that the CA certificate has not been included in a revocation list, the validity of the CA certificate has not expired, and the certificate signature has been verified. The root certification authority is responsible for the CA certificate before reporting the certificate to the revocation list in accordance with the root certification authority's commitments in the certificate policy and this certification practice statement on CA certificates.

2.3.3 The root certification authority's financial administration

The certificate services produced by the Digital and Population Data Services Agency, which acts as the root certification authority, 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.

2.4 Interpretation and implementation

2.4.1 Applicable legislation

The root certification authority complies with the valid Finnish legislation in its certificate service activities.

The position of Digital and Population Data Services Agency is prescribed in the act on the Digital and Population Data Services Agency (304/2019).

The root certification authority conforms to the principles of good personal data processing set forth in the Personal Data Act (523/1999) and to the good information management practices of the Act on the Openness of Government Activities (621/1999).

The DPDSA's certificate activities are based on provisions on identification and trust services laid down in 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 (Regulation).

The Digital and Population Data Services Agency's trust services meet the requirements contained not only in the eIDAS Regulation but also in standard EN 319 401 for qualified trust service providers and standard EN 319 411-1 for qualified trust service providers issuing certificates.

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. Where applicable, the provisions of the Tort Liability Act (412/1974) also apply.

2.4.2 Settling of disputes

When granting certificates, the root certification authority is responsible for the CA certificates meeting the requirements set in this certification practice statement and the certificate policy for CA certificates.

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.

2.5 Fees

This section specifies the fees related to the use of a CA certificate issued by the root certification authority.

2.5.1 Issuing and renewing a CA certificate

CA certificates are applied from the Digital and Population Data Services Agency. A certificate is always issued against a new application, following the identification procedure specified in this certification practice statement. The price of the CA certificate is based on the valid annual fee indicated in the Digital and Population Data Services Agency's service price list.

2.5.2 Fees related to the use of a CA certificate

The root certification authority does not separately charge the CA certificate holder for the use of the certificates, the revocation service or a public directory. The price of the CA certificate is based on the valid annual fee indicated in the root certification authority's service price list.

Individual online service providers may charge a separate fee for the use of their services.

2.5.3 Fees related to the revocation of a CA certificate

Reporting a CA certificate to the revocation list is free of charge. Retrieving revocation lists (ARL) from the directory and checking the validity of CA certificates against the revocation list are also free of charge.

2.6 Publishing and availability of data

2.6.1 Publication of CA certificate data

The root certification authority publishes all CA certificates and revocation lists in a non-chargeable, openly available public directory. The Digital and Population Data Services Agency publishes the Certificate Policy, the Certification Practice Statements, the PDSs and other public documents pertaining to the production of certificate services on its website.

2.6.2 Publication frequency

The CA certificate is published in a public directory where it will remain accessible for the duration of its validity. The root certification authority publishes a revocation list that is valid for one year after its publication. This revocation list is updated once a year or as necessary with a new one.

2.6.3 Availability of data

Directory and revocation list data are publicly available. The FINeID specifications, Certificate Policies and Certification Practice Statements published by the Digital and Population Data Services Agency can be accessed on the Centre's website.

2.6.4 Repositories

The data published by the Digital and Population Data Services Agency is available on the Centre's website. Any non-public certificate system data is saved in the Digital and Population Data Services Agency's own repository. A root certification authority's data is archived according to the authority's valid archiving rules. Particular attention is paid to the processing of personal data and

the Digital and Population Data Services Agency has published specific policy rules conformant to the Personal Data Act on the production of certificate services. The Digital and Population Data Services Agency 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.

2.7 Information security audit

2.7.1 Audit frequency

As a root certification authority, the DPDSA carries out information security audits on the facilities, equipment and operations of its technical suppliers as appropriate. An audit is carried out at least once a year and at the start of each new contract period. In its audit procedure, the Digital and Population Data Services Agency adheres to the practices set out in the ISO 27001 information security management standard.

Audits are carried out to determine the certification authority's compliance with the agreement, taking into account the requirements of information security management standards. Certificate authorities are generally assessed on the basis of ISO 27001.

Finnish Transport and Communications Agency (Traficom), which supervises certification authorities, may audit the operation of a certification authority under the prerequisites set forth in the Act on Strong Electronic Identification and Trust Services.

2.7.2 Auditor

Digital and Population Data Services Agency's information security audit is carried out by Digital and Population Data Services Agency's Head of Information Management or an external auditor specialised in auditing technical vendors pertaining to certificate services.

2.7.3 Audit objects and scope

The objects of the audit are determined by the Act on Strong Electronic Identification and Trust Services or, if Digital and Population Data Services Agency is carrying out the audit, the information security standard ISO 27001, Digital and Population Data Services Agency's information security policy or the technical terms of delivery.

The audit is carried out considering the implementation of the eight areas of information security. Audited information security properties include confidentiality, integrity and availability.

In the audit, the certificate policy, the certification practice statement and the operating instructions of technical suppliers are compared regarding the operations of the entire certificate organisation and system. The Digital and Population Data Services Agency ensures that the operating instructions are consistent with the certificate policy.

In audits, attention is paid to information security in administration as well as various service providers, for example, on the basis of the following categories:

Revocation service:

- communications security
- human resources security
- physical security

Certificate production:

- task allocation and personal tasks – human resources security
- physical security
- security related to the certification authority's private key
- the certification authority's production system and the backup system
- communications security

Card production:

- the production line as a whole from end to end
- quality control of card production
- communications security
- human resources security
- physical security

Directory service:

- components used
- control connections
- directory maintenance and operation in fault situations
- human resources security
- communications security
- physical security

2.7.4 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.

2.7.5 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.

2.8 Publication of data

2.8.1 Information published by the root certification authority

The data in the certificate system will not be published or disclosed unless the disclosure of data is based on the regulations on information disclosure set forth in the Personal Data Act, the Act on the Openness of Government Activities, the Act on the Population Information System and on the Certificate Services of the Population Register Centre or the Act on Strong Electronic Identification and Trust Services or for purposes set forth in the certificate policy or CA certification practice statement.

2.8.2 Public data

The data of the public directory and the revocation list are public, as are the certification practice statements and the data specified in the certificate policy and the published FINEID specifications.

2.8.3 Data pertaining to the expiry or revocation of a CA certificate

The start and expiration date/time of the validity period of a CA certificate are stored in the certificate. CA certificates revoked during their validity period are published on a publicly available revocation list.

2.8.4 Data disclosed to authorities

The data disclosed to authorities is specified according to the valid legislation.

2.8.5 Other data

The data of the CA certificate system are not disclosed for purposes other than those listed above in this section.

2.8.6 Other principles concerning disclosure of information

In terms of the certification authority's reliability, it is essential that the root certification authority takes all possible measures to see to the secrecy of confidential material it obtains in connection with the certificate activities and to the good administration of data unless otherwise required by legislation pertaining to the right of authorities to obtain information on the operation of the certificate system.

Digital and Population Data Services Agency conforms to the Personal Data Act and specific legislation in the processing of personal data. The Digital and Population Data Services Agency has prepared policy rules for the processing of personal data in connection with both information disclosure and with the certificate activities. Special care must be taken when processing personal data.

2.9 Intellectual property rights

The Digital and Population Data Services Agency owns all data pertaining to the certificates and documentation as stated in the technical terms of delivery. Digital and Population Data Services Agency has full ownership and utilisation rights to this certification practice statement and CA certificate policy.

3 Identification of CA certificate applicant

3.1 Registration

Sections 4.1–4.3 present the procedures and processes that are adhered to in the identification and authentication of CA certificate applicants.

The rights and responsibilities of a CA certificate applicant are stated in the agreement on CA certificate provision between the root certification authority and CA certificate holder organisation.

The agreement clearly states that the CA certificate applicant accepts the creation of the CA certificate and its publication. At the same time, the applicant accepts the rules and terms pertaining to the use of the CA certificate as well as the careful storage of the private key and the reporting of any misuse or lost keys.

A CA certificate applicant is responsible for ensuring that all information given by them to the certification authority or registration authority essential for the certificate is correct.

3.1.1 Naming policies

The DPDSA's root certificate authority is:

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

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

3.1.2 Delivery of private keys to the CA certificate holder

The CA certificate applicant creates a private and public key. The CA certificate applicant is obligated to store their private key in a secure environment and prevent its loss, disclosure to outsiders, modification or unauthorised use.

3.2 Renewal of key pair

When renewing CA certificates, the same procedures should be followed as when applying for a CA certificate for the first time. When a CA certificate holder renews their private key, re-registration, a new agreement and a new CA certificate are always required.

3.3 Identification of the requester of revocation

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

Revocation request procedure

A representative of the CA certificate holder organisation must notify the root certification authority immediately if it knows or suspects that the CA certificate's private key has been compromised. The root certification authority will then revoke the relevant CA certificate. Revocation requests are primarily made by the CA certificate holder organisation if the certificate may have been misused. Revocation requests can also be made by the registration authority or the root certification authority.

4 Operational requirements

4.1 Applying for a CA certificate

The rights and responsibilities of a CA certificate applicant are stated in the application document and the agreement concluded with the organisation applying for the CA certificate. The agreement is signed by an authorised representative of the certificate holder organisation. The agreement states the rights and obligations of both parties. It is clearly stated in the application document and the terms of use that by signing the application, the CA certificate applicant confirms the correctness of the information provided and approves the creation of the certificate and its publication in a public directory. At the same time, the applicant accepts the fact that the certificate will be reported to the revocation list if there is a possibility of it being misused.

4.2 Issuing a CA certificate

The root certification authority issues the CA certificate when accepting the application for a CA certificate and signing a related supply agreement on the CA certificate.

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

4.3 Receiving a CA certificate

Once the CA certificate has been issued, it will be delivered to the customer as agreed.

4.4 The validity and revocation of a CA certificate

4.4.1 Prerequisites for revoking a CA certificate

The CA certificate holder must notify the root certification authority immediately if it knows or suspects that the CA certificate's private key has been compromised. The root certification authority will then revoke the relevant CA certificate. An authorised representative of the CA certificate holder organisation has been determined in an agreement between the root certification authority and CA certificate holder organisation.

CA certificates are revoked immediately after receiving a revocation request and after the revocation of the CA certificate has been confirmed.

4.4.2 Requester of revocation

Revocation requests are primarily made by a representative of the certificate holder organisation if the CA certificate may have been misused. A CA certificate may also be revoked by the registration authority or the root certification authority.

4.4.3 Revocation transaction

The CA certificate holder organisation is responsible for revoking the CA certificate. Upon the certificate holder organisation's notification, the CA certificate can be placed

on the revocation list to prevent the use of the CA certificate issued by a root certification authority.

A CA certificate is revoked by notifying the Digital and Population Data Services Agency in accordance with the supply agreement concluded with the CA certificate holder organisation at kirjaamo@dvv.fi. The liability of the CA certificate holder organisation regarding the root certification authority in accordance with the agreement ends upon receipt of an identifiable notification that enables the revocation. The CA certificate holder's liability for the use of the CA certificate ceases at the same time.

Revoked CA certificates cannot be reinstated.

The Digital and Population Data Services Agency will revoke the CA certificates it has issued if an error is detected in the data contents of the certificate or it is known that the private key of a CA certificate has been compromised or there is justified thread thereof, or if there has been failure to comply with the agreement concluded with the CA certificate holder organisation or the agreement has expired.

As the root certification authority, the Digital and Population Data Services Agency may revoke CA certificates signed with its private key if there is reason to believe that the root certification authority's private keys have become disclosed or accessed by unauthorised parties.

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

If the private key used by the root certification authority in issuing a CA certificate or another technical method has become exposed or otherwise unusable, the Digital and Population Data Services Agency must duly notify all CA certificate holder organisations and end users.

The root certification authority may also revoke a CA certificate for other special reasons.

4.4.4 Timing of a revocation event

CA certificates are revoked immediately after receiving a revocation request.

4.4.5 Temporary interruption of the validity of a CA certificate

CA certificates cannot be temporarily suspended.

4.4.6 Publishing frequency of the revocation list

The CA certificate is published in a public directory where it will remain accessible for the duration of its validity. The root certification authority publishes a revocation list that is valid for one year after its publication. This revocation list is updated once per year with a new one.

The revocation list contains the time of publication of the next revocation list.

The new revocation list will be published by the expiration of the validity of the valid revocation list.

In case of system updates and other exceptional situations, DPDSA may publish revocation lists at a different frequency and extended validity periods.

4.4.7 Revocation list requirements

The obligations of a party trusting the CA certificate are described in section 2.

4.4.8 Online CA certificate status check

The CA certificates may only be revoked in the manner described in the agreement or this certification practice statement by visiting the registration authority. The root certification authority does not provide an online certificate status check service that implements OCSP. The certification authority publishes a revocation list of revoked certificates.

4.4.9 Special requirements pertaining to the exposure of the CA certificate holder's private key

It is the CA certificate holder's responsibility to protect the use of their private key by taking all measures for looking after their private key as described in the instructions for use. The CA certificate holder organisation must immediately contact the root certification authority if it suspects that the certificate may have been used in breach of the terms and conditions.

4.5 System supervision

For supervision purposes, the root certification authority stores log data on CA certificate production events, the CA certificate system's access management, the hardware configuration as well as system and application software and their modifications, backup runs and recoveries. In addition, the root certification authority supervises documents related to the activity. Any non-conformances will be reported as agreed with the partner.

4.6 Archiving of data pertaining to CA certificates

4.6.1 Material stored

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 CA certificates, the provisions pertaining to archiving in electronic services legislation are also applied. Backup copies are stored in a place physically separate from the original data.

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

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

The data in the certificate register based on the Act on Strong Electronic Identification and Trust Services is stored for 10 years after the expiry of the CA certificates.

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

4.6.2 Protection of archives

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

Archived data are stored on secure premises with access control.

4.6.3 Backup methods for archived data

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

4.6.4 Acquisition and backup methods for archived data

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

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

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

4.7 Continuity management and handling of deviations.

The root certification authority has a continuity and preparedness plan that enables the continuity of the root certification operations.

4.7.1 The root certification authority's private key has become disclosed or the root certification authority's 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 4.8 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 in accordance with Chapter 6.

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

4.7.2 Compromised security because of a natural disaster or other catastrophe

The security policy of the Digital and Population Data Services Agency, which acts as the root certification authority, 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, setting the requirements for Digital and Population Data Services Agency's operations also after the occurrence of a catastrophe. The Digital and Population Data Services Agency complies with established data security procedures when issuing and administering certificates.

4.8 End of the root certification authority's operation

A situation where all services related to issuing, maintaining and administrating root certification authority and CA certificates are permanently terminated is deemed the termination of the root certification authority. The termination of the root certification authority does not refer to a situation where the root certificate service is transferred from one organisation to another.

The root certification authority communicates the termination of the certificate services to the parties specified in section 4.7.1 a as soon as possible, however at least one month before the time of termination.

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

a) All CA 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 CA certificate has expired.

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

c) c) The root certification authority ensures that access to the root certification authority's archives as set forth in section 4.6 will be maintained also after the termination of the root certification authority.

5 Physical, operational and staff security requirements

An information security certificate has been granted to the root certification authority in its role as a certification authority. The DPDSA's information security solutions meet ISO 27001 requirements.

The root certification authority may use technical vendors for carrying out the information technology tasks of the CA certificate service. The root certification authority is responsible, as the certification authority, for the safety and operation of certificate production in an appropriate way in all of its areas.

The root certification authority follows good information management practices. Services related to certificate provision are organised as certification services of the DPDSA in accordance with the Centre's organisation structure.

5.1 Arrangements related to physical security

5.1.1 Location and building properties

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

The root certification authority's facilities security is implemented by preventing unauthorised entry with appropriate locking systems and the use of suitably solid and durable structures. Data centres have limited windows, and structures are made with durable construction materials.

5.1.2 Physical access to facility

The facilities of the root certification authority where production duties for the authority's 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.

5.1.3 Electricity supply and air conditioning

The data centre facilities for the certification system of the root certification authority have an appropriate air conditioning system. Built-in backup power solutions are in place to protect against unexpected power cuts.

5.1.4 Fire safety

The data centre facilities for the root certification authority's certification system are fitted with the necessary fire alarm mechanisms, first-aid fire-fighting equipment, and automatic fire extinguishers.

5.1.5 Data storage

The root certification authority's archive data and backup copies are stored separately away from the root certification authority's hardware systems.

The root certification authority's data are protected against loss, modification and unauthorised use.

5.1.6 Handling of redundant data

The root certification authority's classified data are destroyed using reliable techniques.

5.1.7 Water damage

The data centre facilities for the root certification authority's certification system are fitted with appropriate humidity detectors.

5.2 Operational requirements

5.2.1 Division of responsibility

The root certification authority uses technical vendors for the registration and information technology duties of certificate production.

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

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

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

5.2.2 Number of staff required for the duties

The creation, activation, backup and recovery of the root certification authority's private keys require the presence of two persons with administrator privileges. The revocation of the root certification authority's private key is possible only under the supervision of two authorised persons. At least two persons authorised to carry out maintenance on the system are present when the certification authority's cryptographic module is initialised.

5.2.3 Task-specific identification

The registration authority of the CA certificate: The unit of the Digital and Population Data Services Agency registering the certification activity serves as the registration authority.

The administrator of the root certification authority's certification system: The administrator of the system is identified on the basis of a personal system management card for the root certification authority. The root certification authority's certification system administrators include the system specialists of the certificate system supplier and authorised personnel of DPDSA.

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

5.3 Personal security

The Digital and Population Data Services Agency serves as a root certification authority responsible for the root certification authority's 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 personnel of the DPDSA's Certificate Service are required to have the necessary educational qualifications and knowledge of certificate operations. Experts monitor industry developments in Finland and Europe and serve as industry experts.

During the contract procedure, the root certification authority has assessed the competence of its technical suppliers' key personnel and employees with regard to the implementation of the root certification authority's certificate service. ICT suppliers maintain the competence of their personnel with regard to the hardware, software, methods and data security used as part of the service provision. In addition, technical suppliers ensure that their personnel are familiar with the data-processing tasks of the certificate service as required by the service.

5.3.1 Carrying out a background check on the staff

Digital and Population Data Services Agency has a basic security clearance done for its staff and technical vendors who work with the CA certificate environment. The checks are carried out by the Finnish Security Intelligence Service. The DPDSA reserves the right to reject a technical supplier's employee from a role that involves working with the root certification authority's certificate system.

5.3.2 Procedure adhered to in the security clearance

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

All relevant personnel of the root 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 a request for a declaration of accountability for the purposes of the declaration of accountability procedure;

- 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.

5.3.3 Training requirements

The root certification authority'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.

5.3.4 Maintenance of expertise and skills

The Digital and Population Data Services Agency's 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.

5.3.5 Requirements for task rotation

When planning for task rotation in the root 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. In task rotation planning, matters such as data security requirements, confidentiality and the principles of handling personal data (as described in the procedural rules regarding the handling of personal data) are taken into account. Task rotation also adheres to root certification authority's information security policy and information security plan as well as the root certification authority's other general instructions.

5.3.6 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).

5.3.7 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 CA certificate services.

5.3.8 Documents given to the staff

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

6 Technical security arrangements

6.1 Generation and storage of key pairs

6.1.1 Generating key pairs

Each root certification authority's key is created on the basis of a random number input which is sufficiently long or generated in a way that makes it impossible to trace back computationally even if the time of creation and the device used to create it are known. In addition, the algorithm and method used to generate the random number meet the qualitative requirements, which include e.g. the reliability of the algorithm, the non-repeatability of the generation method, and the genuine randomness of the random number. The root certification authority will not publish the probability accuracy or method.

Root certification authority:

The root certification authority generates its private signature keys and corresponding public keys. The keys are stored in key management devices governed by the root certification authority. The security level of the key management devices fulfils the criteria required for producing a qualified certificate.

6.1.2 Delivery of a private key to CA certificate applicant

The CA certificate applicant creates its own private and public key.

6.1.3 Delivery of the CA certificate applicant's public key to the root certification authority

The CA certificate applicant shall submit to the registration authority a certificate request it has generated, and the CA certificate will be created on the basis of this request.

6.1.4 Distribution of the root certification authority's public key to the CA certificate holder

The root certification authority's public key is held in the CA certificate, which is freely distributable and also available in the public directory and on the root certification authority's online service.

6.1.5 Key lengths

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

The CA certificate holder's private and public key are 4096-bit RSA keys.

6.1.6 Intended use of keys

The key usage field in the certificates specifies the intended use of the public and private keys associated with a CA certificate (for example, signing of certificates and signing of revocation lists).

The root certification authority's certificate:

Purpose: Signing of CA certificates and revocation lists.

6.2 Protection of private key

6.2.1 Standards for the hardware security module

The root certification authority's private keys are stored in hardware security modules administered by the root certification authority, which meet the requirements of the necessary security standard.

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

6.2.2 Staff participating in the handling of the root certification authority's private key

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

6.2.3 Disclosure of private key to a trusted party

The CA certificate holder organisation must store their private key in a secure environment and prevent its loss, disclosure to outsiders, modification or unauthorised use.

6.2.4 Backup of a private key

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

6.2.5 Archiving of private keys

The root certification authority's private keys are stored in key management devices administered by the certification authority.

The CA 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.

6.2.6 Administration of private keys in hardware security modules

The root certification authority's private signature keys are protected with physical and logical security measures of high reliability. They are only used in a system that operates in a secure environment. The use of keys is controlled with management cards which are protected against unauthorised use.

The root certification authority's employees who work in trusted roles have a PIN-protected management card. The management cards are used to verify the user's access privileges to the certificate system or other related systems.

When a root certification authority's key is no longer in use, the key is destroyed in such a way that it cannot be retrieved or regenerated. Backup copies of the key are destroyed at the same time. The disposal of broken devices is organised in such a way as to reliably destroy private keys from both hardware and software (e.g. by a sufficient number of overwrites).

6.3 Other key management issues

6.3.1 Public key archiving

The root certification authority archives all public keys it has certified.

6.3.2 Usage period of public and private keys

The validity period of a CA certificate is specified in the certificate provision agreement. A CA certificate can be revoked before its expiry if the terms and conditions of the agreement are not complied with or there are other specific reasons stated in this certificate practice statement.

6.4 Security requirements pertaining to the use of and access to computers

6.4.1 Hardware security

Only hardware suitable for its purpose is used in the root certification authority's certificate system.

Hardware security has been implemented according to good information management practice, ensuring that in the event of system failure, a backup system can be used without compromising the confidentiality of the system. The availability of spare parts for mission-critical components is ensured.

In service and maintenance processes, access by external personnel to the systems and facilities which are the responsibility of the service production is prevented. Maintenance visits can only be done by technical suppliers who have signed a technical supply agreement and a confidentiality agreement. A list of approved technical suppliers is maintained.

Maintenance visits can only be done under the supervision of a system administrator or another person authorised by him/her.

The root certification authority's certificate system hardware is under 24-hour security monitoring.

6.5 Certificate system life cycle management

In its role as a root certification authority, the Digital and Population Data Services Agency maintains a classification of importance on certificate service objects and systems, their backup copies, priorities and minimum maintenance levels.

6.5.1 Supervision related to developing the system

The development and testing of the root certification authority's certification system are done in a separate test environment. Only tested, functional and approved solutions are transferred to the production system.

6.5.2 Security management

In its role as a root certification authority, 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.

6.6 Telecommunication network security

The root certification authority's telecommunications security is based on the root certification authority's telecommunication network operating as a joined-up entity which is isolated from other telecommunication networks in an appropriate manner, and its critical components are duplicated. Transmitted messages and their senders or recipients cannot be viewed by unauthorised parties without special measures. The network is only used for tasks related to the root certification authority's certificate system. Redundant network services have been disabled. The network is divided into logical sub-components with restricted connectivity between components. Sufficient authentication, access control and non-repudiation procedures are in place.

6.7 Monitoring of the use of the hardware security module

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

The hardware security module cannot be accessed without an ID card which is used to identify the person and verify his/her access privileges. The module cannot be activated without a system user's personal management card.

The presence of two administrator-level persons and their personal management cards are required to create a new user-level privilege. The module collects log data on events.

7 CA certificate and revocation list profiles

7.1 Technical specifications of certificates

The data content of the root certificate is described in the document FINEID S2. The document is available at the root certification authority's website at www.fineid.fi.

7.2 Revocation list profile

The data content of the revocation lists published by the root certification authority is described in the document FINEID S2. The document is available at the root certification authority's website at www.fineid.fi.

8 Specification document management

8.1 Modifications to specifications

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

8.2 Publication and communication

The root certification authority publishes a certificate policy and a certification practice statement, available at the website www.fineid.fi.

The root 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.

8.3 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 root certification authority and CA certificates. The root certification authority's documents may be modified according to the Digital and Population Data Services Agency's internal change policy.

The Digital and Population Data Services Agency communicates on the modifications well in advance of their entry into force on its website.

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

[Yksikkö] / Aarnio Ville

6.5.2021