DIGITAL AND POPULATION DATA SERVICES AGENCY

# CERTIFICATION PRACTICE STATEMENT FOR THE DIGITAL AND POPULATION DATA SERVICES AGENCY'S WELLBEING APPLICATION SERVICES WELLBEING CERTIFICATES

OID: 1.2.246.517.1.10.305.4
OID: 1.2.246.517.1.10.335.4

1.6.2021

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

## Document management

| | |
|---|---|
| Owner | |
| Prepared by | Ville Aarnio |
| Inspected by | |
| Approved by | Mikko Pitkänen |

## Version control

| version no. | what has been done | date/person |
|---|---|---|
| v 1.0 | Version 1.0 | 1.6.2021/VA |

# Table of contents

# CERTIFICATION PRACTICE STATEMENT FOR THE DIGITAL AND POPULATION DATA SERVICES AGENCY'S WELLBEING APPLICATION SERVICES WELLBEING CERTIFICATES

## 1 General

This document describes the requirements set for the Digital and Population Data Services Agency's (hereafter the "Certification Authority") certification functions based on the Public Key Infrastructure (PKI) as well as the scope of application and limits of this document. In addition to this Certification Practice Statement, the principles presented in this document are determined at the practical level in other policy documents supplementing this document.In this document are defined the terms and conditions for wellbeing applications server certificates to guarantee the security of the communications between wellbeing applications. Such applications are for example mobile device applications collecting personal information of the user and delivering it to Kela Omakanta (The Social Insurance Institution of Finland). This document is in compliance with ETSI TS 102 042 v 2.4.1 regarding service certificates. The reference policy employed is the Organizational Validation Certificates Policy (OVCP).

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.

## 2 References

### 2.1.1 Normative references

The construction of the foundations for the Certification Authority's (CA's) PKI was based on the following legislation, standards and guidelines:

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

[2] the 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] FICORA regulation 72/2016;

[7] the Government Information Security Management Board VAHTI 5/2004: Assurance of Critical Central Government Information Systems;

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

The following principles shall apply to document interpretation:

1. Most headings and subheadings of the Certification Practice Statement are based on international standardisation [RFC 3647]. In document interpretation the text shall prevail over headings.

2. A general condition set for the CA shall be that it must meet all the requirements set in this Certification Practice Statement for the CA.

## 2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) shall apply.

[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

# 3 Definitions and abbreviations

## 3.1 Definitions

Asymmetric encryption: In asymmetric encryption there is a pair of keys is used, one of which is public and the other private. A message encrypted with the public key can only be decrypted using the private key of the key pair in question.

Attribute: Information of permanent nature required to specify a professional and their professional rights;

Certificate applicant: An organisation or individual person that applies for a certificate and that is reliably identified during the application process.

Certificate holder (subscriber): An organisation or individual person whose details and public key have been certified by the electronic signature of the Certification Authority (CA) and that holds the private key associated with the certificate.

Certificate information system: An information technology system consisting of certificate systems, telecommunications, the certificate directory and Certificate Revocation List service, advice and revocation service, and certificate and card administration.

The unique object identifier of the Certification Practice Statement is part of certificate information content.

Certificate Policy: A document that describes the principles followed when issuing certificates and the responsibilities of the relying parties. The Certificate Policies published by the Digital and Population Data Services Agency (DPDSA) are accessible by the public. Each Certificate Policy is assigned a unique object identifier.

Certificate Revocation List (CRL): A list of certificates revoked during their validity period and of their revocation times that is electronically signed and published by the Certification Authority (CA). The publication date of the current and subsequent Certificate Revocation List is also specified in the list. All revoked certificates are included in the Certificate Revocation List. NB! See ITU-T Recommendation X.509.

Certificate system: The information technology system used to create certificates, sign Certificate Revocation Lists and publish them in a directory.

Certificate usage and intended use: In this document certificate usage refers to the usage of both the certificate itself and the usage of the keys associated with the certificate. For example, certificate usage for electronic signatures refers to both the usage of a private key for signing and the usage of a public key and certificate for signature authentication.

Certificate: An electronic attestation that links signature authentication data to the signer (subject) and confirms the subject's identity. The certificate contains the unique object identifier of the related Certification Practice Statement.

Certification Authority (CA): An organisation issuing certificates that is responsible for producing certificates and that draws up a Certificate Policy describing its operations as well as a Certification Practice Statement. NB! See Clause 4.1.

Certification Authority certificate: Contains the name of the Certification Authority (CA), its country and its public key.

Certification Authority private key: A private key used to sign certificates issued and Certificate Revocation Lists published by the Certification Authority (CA).

Certification Practice Statement: A description of the manner in which the Certification Authority (CA) implements its Certificate Policy. Each Certification Practice Statement is assigned a unique object identifier.

Directory service: A public internet service providing access to all of the certificates issued by the Certification Authority (CA) as well as the CA's certificates and Certificate Revocation Lists.

Electronic signature: a PKI signature attached to a message that can be used to reliably verify message content and signer identity.

Key pair: A pair of intertwined keys used in public-key cryptography, one of which is public and the other private. The purpose of the keys is specified in the certificate. NB! See Clause 4.3.

OCSP Online Certificate Status Protocol

OVCP Organizational Validation Certificates Policy

PKI Disclosure Statement: A document that discloses critical information about the Certificate Policy and Certification Practice Statement.

Private key: The private part in a key pair used in asymmetric encryption (public-key cryptography). A certificate holder's private key is stored in a secured environment to protect it against unauthorised access.

Public key cryptography: An information security service, such as the electronic identification of persons, produced using public and private keys, certificates and asymmetric encryption.

Public Key Infrastructure (PKI): An information security infrastructure in which information security services are produced using public-key cryptography.

Public key: The publicly-disclosed key in a key pair used in asymmetric encryption. The Certification Authority (CA) provides its electronic signature to verify that a public key belongs to the certificate holder. The public key is part of the certificate data content.

Registration authority: The registration authority verifies the identity of certificate applicants in accordance with the Certificate Policy and Certification Practice Statement on behalf and at the responsibility of the Certification Authority (CA).

Relying party: A party that acts in reliance on certificate information and uses the certificate for a variety of information security services such as the electronic identification of the certificate holder and the verification of electronic signatures. NB! See RFC 3647

Revocation service: The Certification Authority's service where the CA receives certificate revocation requests, revokes certificates and transmits information about certificate revocation to the certificate system.

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

Secure user device: A device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user.

Server certificate for e-services: A file-based certificate intended for uses such as receiving and sending encrypted messages to and from a shared mailbox. The file contains both the certificates and the associated public and private key.

Server certificate: A service certificate used to identify a server and establish an SSL/TLS encrypted connection between servers. Examples of these include certificates intended for web server use that help users verify the server's trustworthiness. A set of information comprising the public key and identifiers of the service provider using the Public Key Infrastructure (PKI) that the Certification Authority (CA) has created and signed using its private key.

Service certificate: A collective term for server and email service certificates.

Wellbeing applications certificate: Wellbeing applications server certificates to guarantee the security of the communications between wellbeing applications. Such applications are for example mobile device applications collecting personal information of

the user and delivering it to Kela Omakanta (The Social Insurance Institution of Finland).

## 3.2 Abbreviations

CA Certification Authority

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSP Certification Service Provider

EEC Elliptic Curve Cryptography

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

LDAP Lightweight Directory Access Protocol

OID Object Identifier

PDS PKI Disclosure Statement

PKI Public Key Infrastructure

DPDSA Digital and Population Data Services Agency

RSA Rivest, Shamir, Adleman  A commonly used public key algorithm, asymmetric algorithm

SSL Secure Socket Layer

TLS Transport Layer Security

# 4 General concepts

## 4.1 Certification Authority

The Certification Authority (CA) is an organisation issuing and producing certificates upon the operations of which certification service users (i.e. subscribers and relying

parties) rely. The CA shall have the overall responsibility for the provision of certification services specified in Clause 4.2. The CA shall be identified in the certificate as the certificate issuer and qualified certificates shall be signed with its private key.

The CA may use other parties to provide components of its certification service. The CA shall, however, always have overall responsibility and must ensure that the requirements set in this document are met. The CA may, for example, subcontract all service components, including the certificate generation service. The key used to sign certificates shall, however, be specified as belonging to the CA and the CA shall remain the bearer of the overall responsibility for meeting the requirements set in this document as well as responsibility for the issue of certificates issued to the public.

The CA shall be the certification service provider issuing certificates and fulfil the following terms and conditions:

- The CA undertakes to comply with the terms and conditions of the Certificate Policy.
- The CA shall draw up the Certification Practice Statement and other policy instructions that supplement the Certificate Policy.
- The CA shall maintain sufficient financial capacities to secure the activities specified in the Certificate Policy and Certification Practice Statement. The CA shall be responsible for certification activity and related risks and require that certificate system providers take appropriate risk management measures to protect themselves against operational risks.
- The CA shall maintain a register of authorised registration authorities.
- Decisions on cross-certification shall be made by the CA in cooperation with other CAs.
- The CA shall be responsible for the lifecycle of key pairs created by it (generation, storage, backups, publication and withdrawal) and the publication of Certificate Revocation Lists.

The CA undertakes to:

1. provide certification, directory and revocation services specified in the Certificate Policy;
2. provide the administration and monitoring functions described in Clauses 4 to 6 of this Certification Practice Statement;
3. reliably identify certificate applicants;
4. issue certificates in compliance with this Certification Practice Statement;
5. comply with existing laws and decrees and regulations and guidelines issued under them and support the rights of certificate users and relying parties;

6. ensure the performance of sufficient independent audits in compliance with the Certification Practice Statement;

7. bear responsibility for the CA's functionality; and

8. comply with all the terms and conditions of the Certificate Policy and this Certification Practice Statement.

The CA may also decide to provide additional functions or services related to the certificate system.

The CA shall be responsible for ensuring that the information contained in certificates is in compliance with this Certification Practice Statement.

## 4.2 Certification services

### 4.2.1 Registration authority

The registration authority acting in compliance with the Certificate Policy must fulfil the following terms and conditions:

- The registration authority undertakes to meet the requirements set in this Certification Practice Statement.

- The registration authority must be authorised and registered by the Certification Authority (CA).

- The registration authority shall be responsible for the identification of certificate applicants.

- The registration authority shall be responsible for the trustworthiness of registration point personnel. The registration authority must obtain sufficient proof of the trustworthiness of employees hired and ensure the continuous trustworthiness of its authorised personnel. The CA shall approve the registration point personnel on the basis of information provided by the registration authority.

The registration authority under the Certificate Policy must undertake to:

1. comply with existing legislation and regulations and instructions issued under it;

2. provide the administration and monitoring functions required under Clauses 4 to 6 of this Certification Practice Statement;

3. perform the certificate applicant identification procedure in accordance with Clauses 4 to 6 of this Certification Practice Statement and the Certificate Policy and submit the applicant's details to the CA for certificate generation;

4. carry out the agreed assignments and support the rights of certificate users and relying parties; and

5. comply with all the terms and conditions of the Certificate Policy and this Certification Practice Statement related to the registration service.

The registration authority may also provide additional functions or services authorised by the CA. The registration authority shall be responsible for all of the registration services provided by it. The registration authority for the service certificate shall be the Digital and Population Data Services Agency.

### 4.2.2 Certificate revocation service

The certificate revocation service shall revoke the service certificates that the certificate holder or Certification Authority (CA) requests to be revoked before the end of their validity period. All revoked certificates shall be included in the Certificate Revocation List.
Reasons for service certificate revocation may include the illegal disclosure or suspected illegal disclosure of the certificate holder's private key.

### 4.2.3 Directory service

The directory service is a public internet service providing access to all of the certificates issued by the CA as well as the CA's certificates and Certificate Revocation Lists. The directory service shall be available online at ldap://ldap.fineid.fi.

## 4.3 Certificate Policy and Certification Practice Statement

### 4.3.1 Purpose

The Certificate Policy is a description produced by the Certification Authority (CA) regarding the procedures and principles to be followed when issuing certificates. The Certification Practice Statement is a more detailed description of the CA's activities.

### 4.3.2 Level of specificity

The Certification Practice Statement provides a more detailed description than the Certificate Policy of the practices implemented by the Certification Authority (CA) regarding the issue and other administration of certificates. It determines how a specific CA meets the technical, organisational and procedural requirements specified in the Certificate Policy.

### 4.3.3 Approach

The Certificate Policy and the Certification Practice Statement are very different from each other in terms of approach. The Certificate Policy is defined independently of the details of a specific Certification Authority's (CA) operating environment, while the Certification Practice Statement is drawn up specifically in accordance with a CA's organisational structure, policies and methods, premises and information technology environment. A Certificate Policy may be defined by a certification service user but a Certification Practice Statement is always defined by a certificate provider.

### 4.3.4 Other Certification Authority statements

In addition to the Certificate Policy and the Certification Practice Statement, the Certification Authority (CA) may also publish other documents pertaining to its activities. Such terms and conditions of use may include a variety of commercial terms and

conditions or documents such as those related to a specific Public Key Infrastructure. Although customers are not necessarily informed about such terms and conditions, they may still be applied to a case.

The PKI Disclosure Statement is a part of the CA's terms and conditions of use related to the functioning of the Public Key Infrastructure. The CA should make the PKI Disclosure Statement available to both subscribers and relying parties.

## 4.4 Subscriber and subject

The "subscriber" shall mean a party (organisation or individual person) who applies to the Certification Authority (CA) for certificates and has a contractual relationship with the CA. The "subject" shall mean a party (organisation or individual person) to whom a certificate has been issued. The subscriber bears responsibility towards the CA for the use of the private key associated with the certificate based on a public key, while the subject is the individual that can be authenticated by the private key and that has control over its use.

In the case of certificates issued to individuals for their own use the subscriber and subject can be the same entity. In other cases, such as certificates issued to employees, the subscriber and subject are different. The subscriber can, for example, be the employer and the subject can be an employee.

Within the present document these two terms are used with this explicit distinction wherever it is meaningful to do so, although in some cases the distinction is not always crystal clear.

# 5 Introduction to Certificate Policies

## 5.1 Overview

A Certificate Policy is a description produced by the Certification Authority (CA) regarding the procedures and principles to be followed when issuing certificates. The Certification Practice Statement is a more detailed description of the CA's activities.

The Certification Practice Statement shall apply to the Digital and Population Data Services Agency's (DPDSA's) service certificates. The service certificate is a certificate issued by the DPDSA that is used for the certification of a service provider's (organisation's or private individual's) server or service.

The certificate is a set of information that associates the authentication data in conjunction with authentication or encryption with the certificate holder and verifies the service certificate holder. The information in the certificate is electronically signed using the CA's private key. Certificates issued under this Certification Practice Statement shall be based on the Public Key Infrastructure (PKI).

Server certificates may be used for the identification of services. The server certificate shall enable the service user to verify the authenticity of the service provider.

The DPDSA's Certification Practice Statement shall have its unique object identifier (OID). The CA's functions shall include certificate, directory and revocation service

provision and registration. See Clause 4.2 for a more detailed description of these functions.

## 5.2 Identification

A certificate shall have two object identifiers (OID). One of them shall specify which ETSI TS 102 042 Certificate Policy is applied to the certificate and the other one shall be the unique OID for the Certification Practice Statement.

The Certificate Policy shall also have the DPDSA's own OID that determines the Certificate Policy.

The OIDs shall be as follows:

The OID for the ETSI TS 102 042 policy applied (OVCP): 0.4.0.2042.1.3 [itu-t(0), identified-organization(4), etsi(0), other-certificate-policies(2042), policy-identifiers(1), ovcp (7)];

the OID for the Certification Practice Statement for DPDSA's wellbeing applications server certificates:1.2.246.517.1.10.305.4 and 1.2.246.517.1.10.355.4.

the OID for the Certificate Policy for the DPDSA's service certificates: 1.2.246.517.1.10.305 and 1.2.246.517.1.10.355.

The Certificate Policy, its PKI Disclosure Statement and Certification Practice Statements are available online at www.fineid.fi.

## 5.3 User community and applicability

The intended use of server certificates issued in accordance with this Certification Practice Statement shall be server identification and telecommunications encryption. Certificates can be used in accordance with their intended use without limitations in government applications and services as well as those provided by a private person.

The Certificate Policy and Certification Practice Statement contain requirements relating to the obligations of the Certification Authority (CA), registration authority, certificate holders and relying parties as well as to issues related to legislation and settlement of disputes.

## 5.4 Conformance

### 5.4.1 General

The Certification Authority (CA) shall produce certification services under the terms and conditions specified in this Certification Practice Statement and be responsible for their functioning towards the certificate holder. The CA shall be responsible for the functioning of the entire certificate system, including for registration authorities and technical suppliers used. This Certification Practice Statement has been registered by the Digital and Population Data Services Agency. Certificate Policy documents shall be published on the www.fineid.fi website where they shall be accessible by all. The

CA's activities shall be audited every year and whenever major changes take place in the system. Certificate audit reports shall be available on request.

*Information security audits*

The Digital and Population Data Services Agency (DPDSA) shall conduct information security audits of the premises, equipment and activities of its technical suppliers as appropriate.

The DPDSA's information security audits shall be conducted by external auditors that are independent of the Certification Authority (CA).

The audit subject matter shall be determined on the basis of the Act on Strong Electronic Identification and Trust Services (617/2009) or, where the audit is conducted by the DPDSA, on the basis of the ISO 27001 Information Security Management Standard, the DPDSA's information security policy or technical supply agreements. The information security aspects audited shall include confidentiality, integrity and availability.

Audits shall assess the Certificate Policy, Certification Practice Statement and application instructions as well as their compliance with the ETSI TS 102 042 standard regarding the entire certificate organisation and system.

*Measures taken in the event of anomalies*

Any anomalies detected shall be recorded in the audit report and measures in response shall be taken in accordance with legislation, the ISO 27001 Information Security Management Standard and existing supply agreements.

*Provision of information about audits*

Information about audit results shall be provided in accordance with legislation, the ISO 27001 Information Security Management Standard, the DPDSA's information security policy and existing supply agreements. Intended for internal use, the detailed fixed-form audit result shall be confidential and no details of it shall be published. The fixed-form reports shall be drawn up separately for use outside the organisation.

*Archiving of audit material*

The Certification Authority (CA) shall archive the audit reports and minutes, including information security audits and system audits. Archived information shall be retained in accordance with the provisions that apply to the authority acting as the CA.

Plans and policies regarding the CA's activities as well as the CA's obligations in the event of an incident or disturbance are described in Clause 7.4.8. 'Business continuity management and incident handling'.

### 5.4.2 Conformance requirements

The Certification Authority's (CA's) obligations are described in Clause 6.1. The CA's activities shall meet the obligations as defined in Clause 6.1. The CA's activities and controls shall also meet the requirements specified in Clause 7.

# 6 Obligations and liability

## 6.1 Certification Authority obligations

The Certification Authority (CA) shall be responsible for the functioning of the entire certificate system, including for registration Authorities and technical suppliers used.

- It is the statutory duty of the Digital and Population Data Services Agency (DPDSA) to act as the CA.
- The CA shall act in compliance with current legislation.
- The shall CA act in a careful, trustworthy and appropriate manner.
- The CA shall have sufficient technical skills and financial resources for the appropriate performance of certification activity and to cover any liability for damages.
- The CA shall be responsible for all elements of certification activity, including the trustworthiness and functioning of the services and products provided by technical suppliers or individuals used by the CA.
- The CA shall formulate and maintain a Certificate Policy that describes the procedures, terms and conditions of use, division of responsibilities and other aspects of service certificate use applied in the issue, maintenance and administration of service certificates on a general level.
- The CA shall draw up and maintain Certification Practice Statements that describe how the CA applies its Certificate Policy.
- The CA shall meet the requirements set in the Certificate Policy and Certification Practice Statement.
- The CA shall publish the Certificate Policy and Certification Practice Statement and make them accessible by the public.
- The CA shall employ a sufficient number of personnel who possess the expert knowledge, experience and qualifications necessary for the provision of certification services.
- The CA shall use trustworthy systems and products that are protected against unauthorised access.
- The CA shall make information regarding certificates and certification activity, on the basis of which the CA's activities and their trustworthiness can be assessed, available to the public.

Registration authority obligations

The registration authority for service certificates shall be the Digital and Population Data Services Agency (DPDSA).

- The registration authority shall comply with the Certificate Policy and Certification Practice Statement with regards to registration.

- The registration authority shall reliably identify the service certificate applicant in the manner specified in the Certification Practice Statement so that the applicant's identity, right to apply for a service certificate and other applicant details necessary for the issue of the service certificate are carefully checked.

- The registration authority shall ensure the careful handling and confidentiality of data.

- The registration authority shall comply with the registration-related procedures agreed with the CA.

## 6.2 Subscriber and certificate holder obligations

- The service certificate holder shall be responsible for ensuring that the certificate is used in accordance with the intended uses specified in the service certificate application, the Certificate Policy, Certification Practice Statement and terms and conditions of agreement binding on the certificate holder.

- It is possible that Population Register centre issues a certificate for it´s own purposes. In that case it follows the same requirements than issuing certificates for other organisations.

- The certificate holder (service provider) shall be responsible for the accuracy of the information submitted with the certificate application.

- The certificate holder must store its private key in a secured environment and seek to prevent its loss, unauthorised access, modification or unauthorised use.

- The certificate holder must inform the CA immediately if it is known or suspected that the certificate holder's private key has been illegally disclosed or its data content is inaccurate. This shall result in the revocation of the certificate by the CA and the same private key no longer being usable for the generation of new certificates.

- The certificate holder's liability for certificate use shall end as soon as the certificate holder has provided the CA with the information necessary for certificate revocation and been informed of the revocation by the person who received the telephone call. To terminate liability, the revocation notification must be made as soon as the need arises.

All service certificates issued using the illegally disclosed key and valid at the time shall be revoked by inclusion in one or more Certificate Revocation Lists the validity of which shall not terminate until the termination of the validity of the last revoked service certificate.

If a private key or other technical method used by the Digital and Population Data Services Agency (DPDSA) has been compromised or otherwise become unusable,

the DPDSA must inform all certificate holders and Traficom of the situation in the appropriate manner.

The service certificate applicant must provide the registration authority with a certificate request generated using its server to be certified on the basis of which the service certificate shall be generated.

The CA's private key and the corresponding public key shall be 4096-bit RSA keys.

The private and public key length for the service certificate can be decided by the certificate applicant. The DPDSA recommends that the minimum key length used be 2048-bit.

## 6.3 Relying party obligations

Relying parties shall be obliged to ensure that certificates are used for their intended use.

Relying parties must comply with the Certificate Policy and the Certification Practice Statement.

A relying party may rely upon a service certificate in good faith once it has verified that the certificate is valid and that it is not in a Certificate Revocation List (CRL). The relying party is obliged to verify whether a certificate is in a CRL. To ensure reliable service certificate validity, relying parties must comply with the CRL verification measures presented below.

If a relying party retrieves the CRL from the directory, it must verify the authenticity and integrity of the CRL by verifying the electronic signature of the CRL. The period of validity of the CRL must also be checked.

If the latest CRL cannot be accessed from the directory due to equipment or directory service malfunction, no certificate may be accepted if the period of validity of the latest obtained CRL has expired. Any certificate acceptance that takes place following this period of validity takes place at the relying party's own risk.

## 6.4 Liability

*Certification Authority's liability*

The Digital and Population Data Services Agency (DPDSA) shall comply with current Finnish legislation in its certification services.

As the Certification Authority (CA), the DPDSA shall be responsible for the security of the entire certificate system. The CA shall be responsible for services commissioned by it in the same manner as if the service had been produced by the CA itself.

The DPDSA shall be responsible for ensuring that service certificates are generated in compliance with the procedures specified in the Certificate Policy and the Certification Practice Statement and in accordance with the information provided by the certificate applicant. The DPDSA shall only be responsible for information recorded by the DPDSA in the service certificate.

The DPDSA's liability for damages related to the provision of certification services shall be determined in accordance with the provisions of the Tort Liability Act (412/1974). The CA's liability for damages as laid down in the Act on Electronic Services and Communication in the Public Sector (13/2003) shall also apply to the DPDSA.

The DPDSA shall be responsible for ensuring that the service certificate is available from the time of issue throughout its period of validity unless the certificate has been included in a Certificate Revocation List (CRL).

The DPDSA shall be responsible for ensuring that the service certificate has been issued to an applicant that has been identified as required for service certificates.

When signing the service certificate with its private key, the CA shall assure it has verified the information that the certificate contains in accordance with the procedures specified in its Certificate Policy for service certificates and the Certification Practice Statement.

The CA shall be responsible for ensuring that the correct service certificate is placed in the CRL and that it appears in the CRL within the period of time specified in the Certification Practice Statement.

*Registration authority's liability*

The service certificates shall be registered by the Digital and Population Data Services Agency (DPDSA) or its contractual partner on behalf of and at the responsibility of the DPDSA.

*Certificate holder's liability*

The service certificate holder shall be responsible for ensuring that the certificate is used in accordance with the intended uses specified in the service certificate application.

The certificate holder's liability for certificate use shall end as soon as the certificate holder has provided the Certification Authority (CA) with the information necessary for certificate revocation and received a revocation notification from the person who received the phone call. To terminate liability, the revocation notification must be made as soon as the need arises.

*Relying party liability*

A relying party cannot rely upon the accuracy of a certificate in good faith if the validity of the certificate has not been verified from the Certificate Revocation List (CRL). Service certificate acceptance in such cases shall release the Digital and Population Data Services Agency (DPDSA) from liability. A relying party must verify that the certificate issued matches its intended use in the functions for which it is used.

*Limitations of liability*

The Digital and Population Data Services Agency (DPDSA) shall not be liable for any loss, damage or costs arising from the illegal disclosure of the certificate holder's private key unless such disclosure is directly attributable the DPDSA's action.

The DPDSA's liability shall not exceed direct loss or damage to the certificate holder or relying party where the loss or damage is attributable to direct action by the DPDSA and shall never exceed 15% of the amount of certificate invoicing in the preceding 3 months (share booked for the DPDSA).

The DPDSA shall not be responsible for any indirect or consequential loss or damage suffered by the certificate holder. Furthermore, the DPDSA shall not be liable for any indirect or consequential loss or damage suffered by a relying party or other contractual partner of the certificate holder.

The DPDSA shall not be liable for the functioning of public telecommunication connections or information networks such as the internet nor for the performance of a function being disabled due to non-functioning of hardware or software used by the certificate holder nor for the usage of the service certificate against its intended purpose.

The Certification Authority (CA) shall have the right to further develop the certification service. The certificate holder or relying party must cover their own costs arising due to this. The CA shall not be liable for compensating for the certificate holder or relying party for any such costs arising from the CA's development activity.

The CA shall have the right to suspend the certification service for the duration of amendment or maintenance work. Any amendments to or maintenance work on the Certificate Revocation List (CRL) shall be notified in advance.

The CA shall not be liable for errors in an online service or application intended for end users and based on the certificate or any costs arising from such errors during certificate usage.

The certificate holder's liability for certificate use shall end as soon as the certificate holder or a representative of the certificate holder's organisation has provided the CA with the information necessary for certificate revocation and received a revocation notification from the person who received the phone call. To terminate liability, the revocation notification must be made as soon as the need arises.

# 7 Requirements on Certification Authority practice

The Certification Authority (CA) shall implement the controls that meet the following requirements.

These include the provision of services for registration, certificate generation, dissemination, revocation management and revocation status (see Clause 4.2). Where requirements relate to a specific service area of the CA then it is listed under one of these subheadings. Where no service area is listed, or "CA General" is indicated, a requirement is relevant to the general operation of the CA.

These policy requirements are not meant to imply any restrictions on charging for CA services.

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objectives will be met.

## 7.1 Certification Practice Statement

The Certification Authority (CA) shall draw up the Certification Practice Statement and other policy instructions that supplement the Certificate Policy. The CA shall ensure that the Certificate Policies, Certification Practice Statements and PKI Disclosure Statements are publicly available at www.fineid.fi.

The certificate applicant's rights and obligations are specified in the application document and general terms and conditions of use which form the agreement entered into with the certificate applicant.

The application document and terms and conditions of use shall clearly indicate that, on signing the document, the service certificate applicant accepts the accuracy of the information and the generation of the service certificate and its publication in a public directory. Furthermore, in doing so the applicant shall accept the rules, terms and conditions governing the use of the service certificate and the duty to notify of any misuse or illegal disclosure of the private key.

Certification Practice Statement documents shall be determined and approved by the CA.

The CA shall ensure that its certification activity and practice comply with its Certificate Policy.

The CA's operations shall be audited at least once a year. In these audits the Certificate Policy and Certification Practice Statement shall be viewed against the CA's activities on the whole. The CA shall take the measures required to rectify any deviations detected without delay.

Decisions on any amendments to the Certification Practice Statement shall be made by the CA. The only changes that can be made to an adopted Certification Practice Statement without giving notice are corrections to appearance or typing errors or changes in contact details. The CA shall give at least 30 days' notice of any amendments to the Certification Practice Statement other than those referred to above on its website (www.fineid.fi).

The algorithms and other technical parameters employed in certification activity and certificates are described in Clause 7.2.

## 7.2 Public Key Infrastructure – Key management life cycle

### 7.2.1 Certification Authority key generation

The Certification Authority (CA) shall generate its own private signing keys and the public keys that correspond to its private keys. The CA's private keys shall be stored in security modules administered by the CA that meet the requirements set in the required security standard.

The CA shall ensure that CA private keys remain confidential and maintain their integrity. Backup copies of the CA's private keys shall be made in the manner required for critical information security.

Keys shall be stored in security modules administered by the CA. The security of these modules shall meet the requirements identified in FIPS 140-1 level 3.

The CA's private key used for signing service certificates and the corresponding public key shall be 4096-bit RSA keys and 384-bit ECC keys.

The private and public key length for the service certificate can be decided by the certificate applicant. The Digital and Population Data Services Agency (DPDSA) recommends that the minimum key length used be 2048-bit.

The CA shall generate a new key pair and CA certificate no later than within five years and three months from the expiry of the period of validity of the previous CA certificate. The CA certificate shall be made available in the public directory in accordance with Clause 7.3.5.

The generation of a private key shall require the simultaneous presence or activation of at least two persons.

### 7.2.2 Certification Authority key storage, backup and recovery

The CA shall ensure that CA private keys remain confidential and maintain their integrity.

Keys shall be stored in security modules administered by the CA. The security of these modules shall meet the requirements identified in FIPS 140-1 level 3.

There shall be a backup copy of the CA private key.

Backup copies of the CA private keys as well as their storage shall be subject to the same level of security controls as the original CA private keys in all situations.

Private keys and their backup copies shall be stored under strong encryption in devices that meet the requirements set for critical information security.

### 7.2.3 Certification Authority public key distribution

The Certification Authority (CA) certificate that contains the CA public key can be retrieved from the public directory or service maintained by the CA. The CA shall publish its public key in a publicly available public directory at ldap://ldap.fineid.fi and on its website at www.fineid.fi.

### 7.2.4 Key escrow

The subject's private signing keys shall not be held in a way which provides a backup decryption capability (key escrow) where authorised persons could in certain situations perform decryption by utilising information provided by one or more parties.

### 7.2.5 Certification Authority key usage

The intended use of certificate-associated keys shall be determined in the field specifying the intended use in the certificate information content.

The Certification Authority (CA) certificate shall only be used for the purpose of signing service certificates and related Certificate Revocation Lists. Technical specifications can be found in the FINEID S2 specification.

Following the expiry of a CA certificate, the CA private keys kept in a security module shall be destroyed and may not be reused.

CA private keys shall be stored encrypted in security modules.

Activation of CA private keys shall be carried out by authorised persons in security modules using management cards. Use of CA private keys shall be prevented by authorised persons using management cards or by switching off the power supply to the security module containing the CA's private keys.

The CA shall have the right to transfer CA private keys to another security module to maintain or change the original equipment.

CA private keys shall be destroyed on the expiry of their period of validity. CA private keys may only be destroyed by the CA. CA private keys and their copies shall be destroyed in conjunction with the termination of the CA.

Where necessary, the CA shall generate the certificate holder's key pair. In such cases the certificate and the related key pair shall be delivered to the certificate holder in a manner preventing unauthorised access.

The secure key pair generation and storage process shall prevent the disclosure of the key to those outside the system used to generate the keys.

## 7.3 Public Key Infrastructure – Certificate management life cycle

### 7.3.1 Subject registration

The Certification Authority (CA) shall ensure that evidence of subjects' identification and accuracy of their names and associated data are properly examined and that certificate requests are complete, accurate and duly authorised.

The applicant's official name and other details submitted by the applicant and examined by the Registration Authority shall be used in the naming of the service certificate applicant.

A set of attributes that creates the subject name record for the certificate shall be unique and identify the certificate holder in question. Each service certificate holder organisation must operate under its own name.

A certificate holder's private keys shall be generated on the certificate holder's or its technical supplier's server when the certificate in question is a server or system signing certificate. If the certificate is an email service certificate, the CA shall generate the key pair and certificate and deliver them to the certificate holder.

*Verification of the organisation represented by the certificate applicant*

The certificate applicant's rights and obligations are specified in the application document and general terms and conditions of use which form the agreement entered into with the certificate applicant.

The application document and terms and conditions of use shall clearly indicate that, on signing the document, the service certificate applicant accepts the accuracy of the information and the generation of the service certificate and its publication in a public directory. Furthermore, in doing so the applicant shall accept the rules, terms and conditions governing the use of the service certificate and the duty to notify of any misuse or illegal disclosure of the private key.

An agreement shall have been entered into between the CA and the registration authority and other providers supplying elements of certification services that specifies each party's rights, liabilities and obligations indisputably.

The service certificate applicant shall be responsible for the accuracy of all information relevant to the certificate submitted by the certificate applicant to the CA or registration authority. The service certificate holder shall only use the service certificate for its intended use.

On issuing a service certificate the CA shall also approve the certificate application.

The certificate holder must immediately report the service certificate for inclusion in the Certificate Revocation List (CRL) if the holder suspects that usage in breach of contract has been enabled.

Service certificate applications shall be submitted using a form that can be downloaded and printed out at www.fineid.fi.

Before issuing a certificate, the CA shall verify the applicant's details using sources such as the on line Virre –Register maintained by a governmental authority, National Board of Patents and Registration of Finland. Digital and Population Data Services Agency verifies the ownership of the Domain Name by sending an email message in order to control the ownership. Also to be submitted is a proxy if the certificate applicant (such as an IT contact person) acts on behalf of the enterprise/organisation. The same procedure will be conducted in conjunction with certificate renewal. Central and local public government and church authorities are not verified tin the Virre-register. Internet domain names ending in .fi held by the applicant and details of their management must be made available to the DPDSA during the processing of the application. Other domain names are verified in open network based registers if available or otherwise in a reliable manner. Digital and Population Data Services Agency issues certificates only to IPs or domain names dedicated for services provided by a public authority.

If the applicant is a private individual, the applicant must deliver the service certificate application personally to the CA, in which context the applicant's identity shall be verified by means of an identification document issued by the Police (an ID card, passport or a driving licence issued after 1 October 1990).

Other identification documents accepted are a valid passport or ID card issued by a Member State of the European Economic Area, Switzerland or San Marino, a valid

driving licence issued by a Member State of the European Economic Area after 1 October 1990 or a valid passport issued by another country's authority.

A server certificate is issued for a maximum of 27 months.

Certificate renewal shall take place following the same application procedure as for the original application. The fees charged for certificates shall be based on the annual fee specified in the Digital and Population Data Services Agency's service tariff.

The CA shall issue the service certificate on approval of the certificate application.

On issuing the certificate, the CA shall ensure that the certificate information content is accurate at the time of certificate issue.

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

The service certificate issued shall be delivered to the customer as agreed.

### 7.3.2 Certificate renewal, rekey and update

A certificate must be renewed whenever the certificate holder's details relevant to the certificate's information content change. The holder must in such cases contact the CA and apply for a new service certificate.

If the use of a certificate holder's private key is prevented, the certificate associated with the 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.

The procedure applied to certificate renewal shall be the same as that applied to first-time applications.

Certificate information content cannot be changed after certificate generation. The certificate holder must apply for a new service certificate if changes take place in information relevant to certificate information content.

The procedure applied to service certificate renewal shall be the same as that applied to first-time applications. The renewal of a certificate holder's private key always requires re-registration, a new certificate application and a new service certificate.

### 7.3.3 Certificate generation

Certificate information content is specified in the FINEID S2 specification found at www.fineid.fi.

The Certification Authority's (CA's) private keys shall be stored in security modules administered by the CA that meet the requirements identified in FIPS 140-1 or 140-2 level 3. The CA shall ensure that CA private keys remain confidential and maintain their integrity.

The root CA shall sign the CA certificate, which shall be placed in the public directory.

Naming procedures:

CN (Common name) = DVV Gov. Root CA – G3 RSA

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

and

CN (Common name) = DVV Gov. Root CA – G3 ECC

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

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

CN (Common name) = DVV Service Certificates - G5R

OU (Organizational unit) = Palveluvarmenteet

O (Organization) = digi- ja vaestotietovirasto CA

C (Country) = FI

and

CN (Common name) = DVV Service Certificates - G5E

OU (Organizational unit) = Palveluvarmenteet

O (Organization) = digi- ja vaestotietovirasto CA

C (Country) = FI

Certificate holder naming procedure for service certificates (compulsory fields):

SERIALNUMBER (Serial Number) = Serial number

CN (Common Name) = Service name

O (Organization) = Organisation's name

L (Locality name) = City, town or municipality

ST (State or province name) = State

C (Country) = FI

Optional fields:

E (Email address) = Email address

OU (Organizational Unit) = Organisational unit

STREET (Street Address) = Street address

PC (PostalCode) = Postal code

DNS (DNS Name) = DNS Name

The CA certificate holder information shall provide unique identification of the certificate holder organisation.

Activation of CA private keys shall be carried out by authorised persons using security calculation equipment management cards.

The CA private keys shall remain confidential and maintain their integrity in the certificate holder's information system. Access to private keys may only take place using internal commands within the information system.

The key in question must be activated with the correct password for a command related to private keys to be performed.

Archived data shall be stored in high-security premises with access control.

The CA certificate that contains the CA public key shall be retrievable from the public directory or service maintained by the CA.

### 7.3.4 Dissemination of terms and conditions

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties.

The CA certificate that contains the CA public key shall be retrievable from the public directory or service maintained by the CA.

The CA shall give at least 30 days' notice of the entry into force of any changes in the Certificate Policy other than those referred to in Clause 8 on its website (www.fin-eid.fi).

The CA shall publish all service certificates and revocation lists in a public directory made publicly available free of charge. The CA shall publish its Certificate Policy, Certification Practice Statements, PKI Disclosure Statements and other public documents related to the provision of certification services on its website at www.fineid.fi.

*Availability of information*

Directory and Certificate Revocation List (CRL) information shall be publicly available. The public FINEID specifications published by the CA shall be available on the CA's website at www.fineid.fi. Certificate Policies and Certification Practice Statements shall also be available on the CA's website at www.fineid.fi.

*Data warehouses*

Information published by the CA shall be available on the CA's website at www.fineid.fi. Confidential information included in the certificate system shall be stored in the CA's own, confidential data warehouse. CA data shall be archived in accordance with current archiving regulations. Particular care shall be exercised in the processing of personal data, and the Digital and Population Data Services Agency (DPDSA) has published a specific Code of Conduct for the provision of certification services in accordance with the Personal Data Act. The CA has also prepared for each section of the certificate system a personal data file description regarding the processing of personal data. The descriptions are published on the CA's website at www.fineid.fi.

### 7.3.5 Certificate dissemination

A certificate shall be published in the public directory as soon as it has been generated and remain in the directory throughout its validity period. The Certification Authority (CA) shall publish a Certificate Revocation List (CRL) that remains valid for two days following its publication. This CRL shall be updated every hour.

Directory and CRL information shall be publicly available at ldap://ldap.fineid.fi.

### 7.3.6 Certificate revocation and suspension

*Certificate revocation and revocation for a fixed period*

The Certification Authority (CA) shall maintain a certificate revocation service. Information about revoked certificates can be reached by OCSP service offered by the CA Information about revoked certificates shall be published using a Certificate Revocation List (CRL) signed by the CA and published in the public directory. Certificates may not be revoked for a fixed period.

The CA shall not inform the certificate holder of certificate revocation.

*Prerequisites for certificate revocation*

A certificate shall be revoked when:

- revocation is requested by the certificate holder;
- the certificate holder's details relevant to certificate information content have changed;

- the private key associated with the certificate has been lost or illegally disclosed;
- the certificate holder organisation has terminated its operations.

The certificate may not be used or attempted to be used once a request for its revocation has been submitted.

*Who can request certificate revocation?*

Certificate revocation can be requested by:

- a representative of the service certificate holder organisation;
- the service certificate holder;
- the CA if the requirements set in Clause 6.2 are met.

*Certificate revocation process*

The certificate holder submits a certificate revocation request to the CA. This shall take place:

1. by phone;
2. by personal visit to the registration point or
3. in writing to the CA.

Certificates are revoked by the CA in official capacity:

- when the certificate holder organisation has terminated its operations.

The following information shall be recorded regarding certificate revocation:

- service certificate identifiers;
- personal details of the submitter of the revocation request;
- organisation of the submitter of the revocation request;
- identification method of the submitter of the revocation request;
- time of the revocation request;
- reason for the revocation request;
- personal details of the recipient of the revocation request;
- any further information submitted by the certificate holder;
- time of illegal disclosure of the key pair, date of termination of the certificate holder organisation's operations, etc;

- personal details of the operator who performed the revocation;
- time of certificate revocation.

The CA shall not send the certificate holder any separate confirmation of certificate revocation. Information concerning certificate revocation shall be retained for 10 years from the revocation date.

*Certificate holder's responsibility to submit a revocation request*

The certificate holder must submit a certificate revocation request without delay if the requirements for certificate revocation specified in Clause 6.2 are met.

*Certificate revocation request processing period*

The CA shall process certificate revocation requests without delay.

Relying party obligation to verify the validity of certificates

Relying parties must check before accepting a certificate that the certificate is valid and has not been revoked.

Relying parties shall be responsible for checking the valid Certificate Revocation List (CRL). A certificate must not be relied upon if the relying party has not checked the CRL or the OCSP.

*Certificate Revocation List publication frequency*

An updated Certificate Revocation List (CRL) shall be published every hour.

The publication date of the subsequent CRL shall be specified in the current CRL. A new CRL may also be published before the planned publication date.

*Maximum period of CRL validity*

An updated CRL shall remain valid for a maximum period of 72 hours. The time of expiry shall be specified in each CRL.

The certificate holder may also decide to have a certificate revoked before its expiry.

*Revocation request procedure*

The certificate holder or the certificate holder organisation's authorised representative must notify the Digital and Population Data Services Agency's Certification Authority Services if it is known or suspected that the certificate holder's private key has been illegally disclosed. The notification shall be submitted by telephone during office hours on (09) 2291 6748, by fax on (09) 2291 6795 or email signed using a qualified certificate issued by the Digital and Population Data Services Agency to kir-jaamo@dvv.fi. The notification must contain the following information: the notifier's

name and organisation, the serial number of the service certificate to be revoked. The CA shall revoke the certificate in question on receipt of the notification. The certificate holder's liability for certificate usage shall end once the certificate holder has submitted a revocation request to the CA and received a confirmation of the revocation (during the phone call, by fax or by email as applicable).

## 7.4 Certification Authority management and operation

The Digital and Population Data Services Agency shall maintain a priority classification regarding certification service objects and systems, their securing, prioritisation and minimum maintenance level.

### 7.4.1 Security management

The Digital and Population Data Services Agency's (DPDSA's) information security management takes place in compliance with the DPDSA's information security policy and the ISO 27001 standard.

### 7.4.2 Asset classification and management

The Digital and Population Data Services Agency (DPDSA) is an agency operating under the Ministry of Finance and the certification services produced by it are covered by the financial management system and supervision governed by specific provisions. The DPDSA's financial management is based on laws and decrees governing central government finances as well as regulations issued by the Ministry of Finance and the State Treasury. Financial supervision is performed by the National Audit Office. Operational performance is also described from the perspective of effectiveness, economic efficiency and productivity.

Under the General Terms and Conditions of Government IT Procurement (JIT 2007) the DPDSA is responsible for ensuring that it has sufficient financial resources for the appropriate performance of certification activity and to cover any liability for damages.

### 7.4.3 Personnel and information security

The Digital and Population Data Services Agency (DPDSA) shall act as the Certification Authority (CA) responsible for certification activity. Technical subcontractors shall have been selected on the basis of competitive tendering and act on behalf and at the responsibility of the DPDSA.

The DPDSA shall pay particular attention to the reliability of both its own personnel and that of technical suppliers and registration authorities as well as the skills needed in the performance of tasks.

*Background checks*

The Digital and Population Data Services Agency shall obtain a basic background check on its own personnel and the personnel of technical suppliers who work in the certificate environment.

*Background check procedure*

Employees' work experience shall be examined during the recruitment process. A basic background check shall be performed on each employee on the basis of the information provided by the person using a standard form.

All those performing critical tasks in the Certification Authority (CA), certification services, directory service provision and revocation service must:

- fill in a form that will be submitted to the Finnish Security Intelligence Service for a basic background check on them;
- abstain from any tasks that are in conflict with their obligations and responsibilities;
- be persons who are not known to have been released from any previous tasks due to neglect of obligations or misconduct;
- be appropriately trained for their tasks.

*Training requirements*

Personnel of the Digital and Population Data Services Agency (DPDSA) shall be trained in a manner ensuring the best possible performance of their tasks. The DPDSA shall have a training plan with the DPDSA's Administration Unit responsible for its implementation.

*Expertise and competence maintenance*

Personnel training shall be planned and maintained in a manner ensuring that the expertise related to the performance of tasks is always at the best possible level as required for each task.

*Job rotation-related requirements*

Where job rotation is planned regarding Certification Authority (CA) duties, tasks must be organised is a manner ensuring the person is capable of performing their new tasks in the best possible manner. Maintenance of good information management practice and sufficient task-specific competence level shall be taken into consideration in job rotation planning.

The DPDSA's information security policy and information security plan and other general guidelines of the DPDSA shall also be complied with in job rotation.

*Measures taken in the event of anomalies*

The personnel of the DPDSA shall perform their duties under the legal liability of a public servant for their official acts in office and in accordance with the DPDSA's internal guidelines. Provisions regarding the status of public servants are laid down under the Public Servants Act (750/1994).

*Personnel representing the organisation*

Personnel recruitment shall take place making sure personnel's skills are in compliance with the requirements set by their duties and that the background check carried

out on them did not reveal anything that might create a conflict between their duties and certificate service provision.

*Documents made accessible by personnel*

The personnel shall always have access to the DPDSA's quality and security documents.

### 7.4.4 Physical and environmental security

The Digital and Population Data Services Agency (DPDSA) uses technical suppliers for the performance of information technology duties related to certification services. As the Certification Authority (CA), the DPDSA shall be responsible for the security and appropriate functioning of all areas of certificate production.

*Location and building properties*

The CA's systems shall be located in high-security data centres and comply with the security guidelines and regulations issued for computer centres.

Premises security shall be ensured through the prevention of unauthorised access to the premises.

*Physical access to premises*

Access to premises where certificate system production duties take place shall be controlled. Both authorised and unauthorised access shall be detected by the access control system. Access to data centre premises shall require identification where the person is identified, his/her access rights checked and the events registered. Data centre premises shall be guarded around the clock.

*Backup arrangements*

Hardware solutions shall have been implemented in accordance with good data management practice to make sure that, in the event of system failure, a backup system can be activated without compromising the confidentiality, integrity or availability of data in the system.

Access to and servicing of spare parts of important hardware shall be secured.

### 7.4.5 Operations management

The Digital and Population Data Services Agency (DPDSA) uses technical suppliers for certificate production registration and IT tasks. The DPDSA shall act as the Certification Authority (CA) responsible for certification activity.

The CA's duties have been divided into the following responsibility areas:

- information security;
- registration;
- system maintenance;

- system usage;
- system control.

A supply agreement has been signed between the CA and the technical supplier, containing a detailed specification of the supplier's tasks, methods and responsibilities and the manner of ensuring information security.

### 7.4.6 System access management

The generation, activation, backup copying and recovery of the Certification Authority's (CA's) private key shall take place in the presence of two persons authorised for system maintenance duties.

A minimum of two persons authorised for system maintenance duties shall be present during the formatting of the CA's private key security module.

The presence of one person authorised for the task shall be required for system usage.

The presence of one person shall be required for service certificate registration and identification.

### 7.4.7 Trustworthy systems deployment and maintenance

Service certificate registration authority: The Certification Authority Services of the Digital and Population Data Services Agency shall act as the registration authority.

Certification system maintenance operators: Operators shall be identified using a personal management card intended for system maintenance. System maintenance operators shall comprise the certificate system supplier's system experts and DPDSA employees authorised for the task.

Certification system users: Users shall be identified using a personal ID card intended for system use. Certificate system users shall comprise data centre operators, technical certificate request launchers and the revocation service.

### 7.4.8 Business continuity management and incident handling

The Digital and Population Data Services Agency (DPDSA) shall have a continuity and preparedness plan that enables the continuity of certification activity.

*CA private key compromise or certificate revocation*

The root Certification Authority (CA) shall specify in each of its Certification Practice Statement the measures to be taken by the root CA, the holders of certificates issued by the CA, parties relying upon the certificates issued by the CA, registration authorities and root CA employees in the event of compromise or other situation where the root CA's private key cannot be used.

In such cases the root CA shall either terminate its operations as described in Clause 7.4.9 or perform the following measures:

a) The root CA shall notify of the event all those holders of certificates issued by the CA, relying parties and all customers with whom the CA has signed an agreement or that are otherwise in such a relationship with the root CA due to their contractual relationship or official activity that they must be informed by the root CA of the issue.

b) The root CA shall generate a new key in accordance with Clause 7.3.3.

c) All CA and end-user certificates issued using the compromised key and valid at the time shall be revoked by inclusion in one or more revocation lists the validity of which shall not terminate until the termination of the validity of the last revoked CA certificate

*Compromise of security due to a natural or other disaster*

The DPDSA security policy shall include provisions for measures to be taken in the event of an external security threat. The DPDSA has been issued with the ISO 27001 Information Security Management Certificate, under which specific requirements are set for DPDSA activities, including in the event of a disaster.

### 7.4.9 Certification Authority termination

Certification Authority (CA) termination shall be a situation where all CA services related to certificate issue are permanently terminated. Situations where a certification service is assigned from one organisation to another shall not constitute CA termination.

The CA shall provide notice of certification service termination as soon as possible and always no later than one month before the date of termination.

Before the CA terminates its services, the following procedures shall be executed as a minimum:

a) The CA shall revoke all issued and valid service certificates by inclusion in one or more Certificate Revocation Lists (CRL) the validity of which shall not terminate until the termination of the validity of the last revoked service certificate.

b) The CA shall terminate all authorisation of its contractual partners to act on behalf of the CA in the performance of any functions related to the process of issuing certificates.

c) The CA shall ensure that access to the CA's archives shall be maintained following the termination of the CA's operations.

### 7.4.10 Compliance with legal requirements

The Digital and Population Data Services Agency (DPDSA) shall comply with current Finnish legislation in its certification services.

Provisions regarding certificates issued by the DPDSA are laid down in the Act on the Population Information System and the Act on Certificate Services Provided by the the Digital and Population Data Service Agency (661/2009).

The DPDSA's liability for damages related to the provision of certificate services shall be determined in accordance with the provisions of the Tort Liability Act (412/1974). The Certification Authority's (CA's) liability for damages as laid down in the Act on Electronic Services and Communication in the Public Sector (13/2003) shall also apply to the Digital and Population Data Services Agency.

### 7.4.11 Recording of information concerning certificates

Information published by the Certification Authority (CA) shall be available on the CA's website. Confidential data of the certificate system shall be stored in the CA's own, confidential data warehouse. CA data shall be archived in accordance with current archiving regulations. Particular care shall be exercised in the processing of personal data, and the Digital and Population Data Services Agency (DPDSA) has published a specific Code of Conduct for the provision of certification services in accordance with the Personal Data Act. The CA has also prepared for each section of the certificate system a description of personal data file regarding the processing of personal data.

The provisions of the Archives Act (831/1994) shall apply as general legal provisions governing archiving. The right to access information shall be determined in accordance with the Act on the Openness of Government Activities (621/1999). Provisions laid down in legislation on electronic services shall also apply to the archiving of certificates. Certificate register data shall be retained for ten (10) years following certificate expiry. The following information shall be archived by the CA:

a) the application form signed by the applicant, a document attesting the receipt of the server certificate and related general terms and conditions of use;

b) server certificates issued, their data content and further information related to lifecycle management since the expiry of their validity period or since their revocation;

c) events related to the generation and renewal of the CA's private key;

d) server certificate revocation requests;

e) Certificate Revocation Lists saved in the public directory and other information related to server certificate revocation;

f) the currently valid and previously published Certificate Polices and corresponding Certification Practice Statements;

g) measures performed by certificate system maintenance and users registered as certificate system users are recorded in log files;

h) audit reports and minutes, including information security audits and system audits.

Archived information shall be retained in accordance with the provisions that apply to authorities acting as a CA of qualified certificates.

*Archives protection*

The CA shall store archived documents related to server certificate retrieval, identification of persons and issue of server certificates in appropriate premises.

Archived data shall be stored in high-security premises with access control.

*Archived data backup procedures*

Backup copies shall be stored in premises that are physically separate from original data.

*Archived data access and backup methods*

In the event of CA service suspension or termination, the CA shall inform all of its customers that the archives will remain accessible. All inquiries concerning archived data shall be sent to the CA or the party specified by the CA before the termination of its operations.

The CA shall ensure archive accessibility and readability, including in the event that the CA's activities are suspended or terminated.

Data from archives may be released as justified from the perspective of the server certificate holder or relying party.

## 7.5 Organisational requirements

The Digital and Population Data Services Agency (DPDSA) is an authority maintaining a personal data file that is tasked in addition to its other duties with the provision of services related to certified e-Government services in accordance with the Act on the Population Information System and the Act on Certificate Services Provided by the Digital and Population Data Service Agency (661/2009).

The DPDSA shall issue certificates on application. The certificate applicant's rights and obligations shall be specified in the DPDSA's certificate application document and general terms and conditions of use which form the agreement entered into with the certificate applicant.

An agreement shall have been entered into between the DPDSA and the registration authority and other providers supplying elements of certification services that specifies each party's rights, liabilities and obligations indisputably.

The certification services produced by the DPDSA are covered by the financial management system and supervision governed by specific provisions. The DPDSA is an agency operating under the Ministry of Finance. The DPDSA's financial management is based on laws and decrees governing central government finances as well as regulations issued by the Ministry of Finance and the State Treasury. Financial supervision is performed by the National Audit Office. Operational performance is also described from the perspective of effectiveness, economic efficiency and productivity.

The DPDSA shall comply with current Finnish legislation in its certification services. The DPDSA shall act in a careful, reliable and appropriate manner. The DPDSA shall make information regarding certificates and certification activity, on the basis of which the CA's activities and their trustworthiness can be assessed, available to the public.

The DPDSA shall pay particular attention to the trustworthiness of both its own personnel and that of technical suppliers and registration authorities as well as the skills needed in the performance of tasks. The DPDSA shall have sufficient technical skills

and financial resources for the appropriate performance of certification activity and to cover any liability for damages. The personnel of the DPDSA shall perform their duties under the legal liability of a public servant for their official acts in office and in accordance with the DPDSA's internal guidelines. Provisions regarding the status of public servants are laid down under the Public Servants Act (750/1994).

Any disputes shall be settled in accordance with Finnish law. Settlement of complaints and disputes and financial supervision and administration of justice shall take place under current legislation.

This Certification Practice Statement has been registered by the DPDSA and the copyright thereto shall be owned by the DPDSA. The DPDSA shall own all information related to certificates and documentation in accordance with the technical supply agreements. The DPDSA shall own full ownership and access rights to this Certification Practice Statement. The DPDSA shall be responsible for the administration of and updates to this Certification Practice Statement.

# 8 Framework for the definition of other certificate policies

This clause provides a general framework for other policies for Certification Authorities (CAs) issuing certificates. A CA may claim conformance to this general framework as defined in clause 8.3. In general terms this requires conformance to the requirements in Clauses 6 and 7 excluding those applicable only to CAs issuing certificates to the public.

## 8.1 Certificate policy management

*Re-specification*

The Certification Authority (CA) may carry out re-specification due to legislative, operational or technical requirements. Any re-specification must be entered in the Certificate Policy and Certification Practice Statement documents as follows.

*Publication and information provision*

The CA shall publish a Certificate Policy and Certification Practice Statement and make them available online at www.fineid.fi.

The CA's public specifications concerning certificate production shall also be available on the same website.

Agreements entered into with IT suppliers regarding certificate supply as well as production system descriptions and product specifications shall be confidential.

*Certification Practice Statement amendment and adoption procedures*

Certificate Policies and Certification Practice Statements for service certificates shall be adopted by the DPDSA. Any changes to these documents may only take place in accordance with the DPDSA's internal amendment procedures.

The DPDSA shall provide a notification of any amendments in good time before their entry into force to the Finnish Transport and Communications Agency (Traficom) and on its own website.

The DPDSA shall perform document version management and archive all Certificate Policy and Certification Practice Statement documents. Typographic corrections and changes in contact details may be made immediately.

1. Amendments to any item of the Certificate Policy and the Certification Practice Statement may be made following a notice of future amendments to main substance given 30 days before their entry into force.

2. Items that the DPDSA does not regard as having a significant impact on certificate holders or relying parties may be amended by giving 14 days' notice.

## 8.2 Additional requirements

Subscribers and relying parties shall be informed, as part of implementing the requirements defined in Clause 7.3.4, of the ways in which the specific policy adds to or further constrains the requirements of the certificate policy as defined in the present document.

## 8.3 Conformance

The Certification Authority (CA) shall only claim conformance to this Certification Practice Statement:

a) if the CA claims conformance to the identified Certificate Policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance. This evidence can be, for example, a report from an auditor confirming that the CA conforms to the requirements of the identified policy. The auditor may be internal to the CA organisation but should have no hierarchical relationship with the department operating the CA; or

b) if the CA has a current assessment of conformance to the identified Certificate Policy by an independent party. The results of the assessment shall be made available to subscribers and relying parties on request.

[Yksikkö] / Aarnio Ville 31.3.2021