CERTIFICATION PRACTICE STATEMENT ORGANISATION CERTIFICATES PERSONNEL

for non-regulated social welfare and healthcare worker's certificate

For Digital and Population Data Services Agency

OID 1.2.246.517.1.10.203.3

ISO 9001

ISO/IEC 27001

DOCUMENT MANAGEMENT	
Owner	
Author	Tuire Saaripuu
Checked by	
Approved by	Joonas Kankaanrinne

VERSION MANAGEMENT		
version no	action	date/author
1.0	Approved version, an eIDAS-compliant document	3 May 2018
1.1	Approved version, Centre name change	1 Jan 2020

Contents

1 Introduction

The prerequisites of the PKI (Public Key Infrastructure) certification activities of the Digital and Population Data Services Agency (hereinafter 'the certification authority') and the application and scope of this document are defined in the certificate policy. The practical implementation of the principles set out in the certificate policy is described in this certification practice statement.

All parties referred to in this certification practice statement (CPS) shall comply with this CPS, the act on the electronic processing of client data in social and health care (159/2007) and the act on electronic prescriptions (61/2007) and associated regulations and requirements.

This document specifies the procedure requirements that apply to certification authorities that grant signature certificates and to Digital and Population Data Services Agency, which is the provider of a strong electronic identification means. Procedure requirements are set for the activities and administration practice of certification authorities that grant certificates so that the subscribers, signers certified by the certification authority and the parties trusting the certificate can trust that the certificate can be used to verify electronic signatures.

The provision of the strong electronic identification means offered by Digital and Population Data Services Agency takes place in the same production environment, with similar technical and functional solutions and subject to the same procedures as with the provision of the signature certificate granted by Digital and Population Data Services Agency.

The purpose of this CPS document is to describe the methods used to ensure the reliability of certificates issued by the Digital and Population Data Services Agency (DPDSA). This CPS defines the procedures of the certification authority and certificate users, and the general security requirements which are in place in order to minimise operational, financial and legal hazards and risks related to public key infrastructures.

A certificate connects a public key with a set of data which identify a subject such as a natural person, an organisation, a website or a device. The certificate is used by the certificate holder and the trusting party, who trusts the validity of the certificate and uses it, for example, to authenticate digital signatures.

The certification practice statement and its application are described in this chapter. In addition, it defines the organisation responsible for the management of the CPS, and its contact information.

1.1 Background

DPDSA issues certificates to regulated healthcare professionals as defined in the Act on Health Care Professionals (559/1994).

DPDSA offers highly secure digital signature and authentication certificates and associated services. Certificates are used to verify the certificate holder's identity and the accuracy, integrity and authenticity of data contained in the certificate. Digital signing based on qualified certificates and identification by strong electronic identification devices enable citizens to access pub-

lic services online securely and flexibly anytime, anywhere. Qualified certificate and strong electronic identification service providers are supervised by the Finnish Transport and Communications Agency (Traficom).

Signature certificates issued under this CPS meet the requirements of the Regulation. Provisions on digital signing using a qualified certificate are set out in the Act on Strong Electronic Identification and Trust Services (617/2009)

As of 1 December 2010, DPDSA is a statutory certification authority in the healthcare sector under the act on the electronic processing of client data in social and health care (159/2007) and the act on electronic prescriptions (61/2007) and the Act on the Digital and Population Data Services Agency (304/2019).

The DPDSA's PKI has been formulated on the basis of statutes, standards and guidelines including:

- The act on electronic prescriptions (61/2007)
- The act on the electronic processing of client data in social and health care (159/2007)
- The act on Health Care Professionals (559/1994)
- The Act on Strong Electronic Identification and Trust Services (617/2009)
- The Act on Electronic Services and Communication in the Public Sector (13/2003)
- The Act on the Openness of Government Activities (621/1999)
- The Act on Background Checks (177/2002)
- IETF RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (11/2003)
- IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (4/2002)
- ETSI TS 101 456, v1.4.3: Policy requirements for certification authorities issuing qualified certificates (5/2007)
- ISO/IEC 17090-3: Health informatics - Digital Certificates in Healthcare - Part 3: Policy management of certification authority
- FICORA Regulation M 72/2016 on Electronic Identification and Trust Services
- VAHTI 1/2002: Information security recommendation for ICT premises
- VAHTI 5/2004: Securing the state administration's key information systems

The following principles apply to the interpretation of this document:

1. The headings and subheading of the CPS are primarily recommendations of international standards [RFC 3647] which have been translated into Finnish. The body of the text takes precedence over the headings.

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

3. The "—" character means that the topic in question is not subject to any additional terms and conditions not defined in the certificate policy.

1.2 CPS identifiers

The title of this CPS is the Certification Practice Statement for non-regulated social welfare and healthcare worker's certificates, OID on 1.2.246.517.1.10.203.3.

This certification practice statement refers to the Certificate Policy for Organisation Certificates, OID 1.2.246.517.1.10.203, and the qualified electronic certificate policy document which is part of the professional certificate.

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 shall apply with regard to signature certificates in trust services as of 1 July 2016. The procedural requirements concerning the activities and administrative practices of certification authorities that issue signature certificates under the Regulation are described in this document. The use of a secure signature creation device is described in the procedural requirements specified in this document.

Digital and Population Data Services Agency adheres to a certificate policy concerning signature certificates issued to the public as per trust services under Regulation No. (EU) 910/2014. The document reference as per ETSI EN 319 411-1 [2], QSCD is: OID: 0.4.0.194112.1.2. Signature certificates issued in accordance with this certificate policy can be used to authenticate digital signatures that correspond to approved certificates and creation devices for digital signatures as referred to in the Regulation and provided for in Articles 28 and 29 of the Regulation. The level of the identification certificate meets the requirements of High level of assurance in accordance with the Regulation and the regulation on levels of assurance.

1.3 Parties and application

The parties that are involved in the provision or use of the certificates or as system suppliers are described in this chapter.

1.3.1 Certification authority

The certification authority meets the following terms and conditions:

- The certification authority agrees to adhere to the terms and conditions set out in this CPS.

- The certification authority draws up a certificate policy and a certification practice statement and other supplementary instructions.

- The certification authority maintains adequate financial resources in order to secure the operations referred to in this CPS. The certification authority is responsible for the certificate activities and the associated risks and requires the certificate system suppliers to take appropriate risk management measures in order to safeguard against risks related to the activities.
- The certification authority maintains a register of its approved registration authorities.
- The certification authority makes decisions on cross-certification in cooperation with other certification authorities.
- The certification authority is responsible for the life cycle of key pairs created by it (generation, storage, backups, publishing and disposal).

The certification authority agrees to:

1. provide certificate and directory services defined in this CPS;
2. provide the management and monitoring functions described in sections 4–6 of this CPS;
3. require the registration point to perform the identification procedure in accordance with sections 3–4 of this CPS;
4. issue certificates in accordance with this CPS;
5. comply with valid acts and decrees and associated regulations and guidelines and support the rights of certificate users and trusting parties;
6. provide a revocation service in accordance with sections 3–4 of this CPS;
7. ensure that sufficient independent auditing is performed in accordance with the CPS;
8. ensure the functioning of the certification authority; and
9. comply with the terms and conditions set out in this CPS and the certificate policy.

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

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

The certification authority audits and approves registration authorities and their personnel.

1.3.2 Registration authority

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

- The registration authority agrees to comply with the requirements set out in this CPS.

- The registration authority must be approved and registered by the certification authority.
- The registration authority is responsible for the identification of certificate applicants.
- The registration authority is responsible for the trustworthiness of the registration point personnel. The registration authority obtains background checks on recruited personnel as required by the certification authority and ensures the trustworthiness of its personnel at all times. The certification authority approves the registration point personnel on the basis of background checks obtained by the registration authority.

A registration authority operating under this CPS must agree to:

1. comply with valid legislation and associated regulations and guidelines;
2. provide the management and monitoring functions specified in sections 4–6 of this CPS;
3. perform the certificate applicant identification procedure in accordance with sections 3–4 of this CPS and the certificate policy;
4. perform the agreed assignments and support the rights of certificate users and trusting parties; and
5. comply with all terms and conditions on the registration service as set out in this CPS and the certificate policy.

The registration authority may offer additional functions or services approved by the certification authority.

The registration authority is responsible for all registration services provided by it.

1.3.3 Certificate holder

Non-regulated healthcare worker's certificates can be issued to persons working in non-regulated positions in a healthcare service provider organisation.

Applicants for the non-regulated healthcare worker's certificate must show proof of identity when making the application.

By signing the certificate application, the applicant agrees to the terms and conditions of use. The applicant receives the current terms and conditions together with the certificate.

1.3.4 The trusting party

The trusting party is an owner of an information system which features security mechanisms that are able to use non-regulated healthcare worker's certificates.

The trusting party is bound by the trusting party's obligations set out in this CPS.

The trusting party agrees to implement in its system all the required components as specified in the certificate policy and CPS (e.g. digital signature verification, certificate path validation, certificate validity verification via the OCSP service or certificate revocation list validation) and modify its system in line with any updates made to the certificate policy or CPS.

1.3.5 Other parties

The certification authority may, at its discretion, use subcontractors and partners who operate in Finland in the provision of the certificate services.

1.4 Uses of the certificate

Typical uses of the certificate which are supported by this CPS are described in this chapter. This CPS applies to the certification authority, registration authorities, certificate holders, and trusting parties.

Non-regulated healthcare worker's certificates are used in national healthcare information systems. National healthcare information systems are systems which are used to execute the duties of the Social Insurance Institution of Finland (Kela) as set out by the act on electronic prescriptions (61/2007) and the act on the electronic processing of client data in social and health care (159/2007). In addition, non-regulated healthcare worker's certificates can be used in other information systems of healthcare and pharmacy services.

1.4.1 Permitted uses

The professional certificate consists of a certificate pair that has two different purposes. The authentication and encryption certificate meets the requirements for a strong electronic identification means. A signature certificate intended solely for implementing a signature meets the requirements on qualified certificates as set out in the Regulation. The correctness of the certificate applicant's identity is guaranteed by Digital and Population Data Services Agency.

This certification practice statement describes the issuing and production of a qualified certificate for digital signatures conformant to the Act on Strong Electronic Identification and Trust Services and detailed requirements pertaining to the division of responsibility.

This document also describes solutions and procedures pertaining to the granting, production and data storage of an identification certificate offered as a means referred to in the Act on Strong Electronic Identification and Trust Services, included in the professional certificate, conforming to the requirements of the production environment of the qualified certificate.

1.4.2 Prohibited uses

Transmission of patient information by email is prohibited in accordance with the decision by the Ministry of Social Affairs and Health. The use of non-regulated healthcare worker's certificates in the encryption or signing of email messages that contain patient information is therefore prohibited.

1.5 Contact details

1.5.1 The organisation responsible for this CPS

This certification practice statement describing the issuance of non-regulated healthcare worker's certificates has been registered by Digital and Population Data Services Agency.

Certification authority's contact details

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

Digital and Population Data Services Agency (DPDSA) Certificate Services

P.O. Box 123

FI-00531 Helsinki

www.fineid.fi

1.5.2 Relationship between certification practice statements and the certificate policy

Certification practice statements (CPS) are maintained in line with the certificate policy (CP). The contents of the CP always take precedence over the CPS. The CP and CPS review processes are specified in chapter 8.

1.5.3 CPS approval process

CPS documents are formulated and approved by the DPDSA Certificate Service.

1.6 Definitions and abbreviations

Professional practice rights, right to practise: In this CPS, 'professional practice rights' and 'right to practise' refer to the professional rights which, under section 2 of the Act on Health Care Professionals (559/1994), are available to licensed and authorised professionals or professionals with a protected occupational title or persons studying for the profession in question. The right to practise may be unlimited, limited or cancelled. Individuals' practice rights are registered in Terhikki, a database maintained by the National Supervisory Authority for Welfare and Health (Valvira).

Key recovery: Key recovery refers to the recovery of a private key if the certificate card is damaged or lost. Private keys of healthcare certificate cards cannot be recovered in the event of card loss or damage.

Key management: Key management refers to the processes and solutions used to manage the CA's keys and the certificate holder's authentication and encryption keys and signature keys

over the keys' life cycle. The stages of the key life cycle are: ordering, generation, distribution, storage, use, revocation, renewal, archiving, and disposal.

Integrity: 1) The authenticity, genuineness, inherent consistency, completeness, currency, accuracy and usability of data or a data system; 2) the notion that a data item or message has not be tampered with and that any changes can be verified from an audit trail.

Public Key Infrastructure (PKI) In a public key infrastructure, the named certification authority produces key pairs for users, verifies them with its digital signature, guarantees the certificate holder's identity, distributes certificates to users, maintains the certificate directory and revocation list, and, if applicable, provides other services related to the PKI. In a PKI, each users has two interconnected keys. One of the keys is public and one is a private key that is only in the user's possession. The authenticity of a data item that has been signed with a private key can only be verified by the corresponding public key, and, conversely, data encrypted with the recipient's public key can only be decoded by the recipient's private key.

Non-repudiation: Non-repudiation means that the parties' involvement in the transaction or activity can be proven afterwards. Non-repudiation ensures that neither party can deny the action, such as the signer having signed something, after the event. The purpose of non-repudiation is legal validity.

Card management application (KoHa): A database application that is operated as a separate component of the certificate system; supports the registration service and revocation service and is used to store data such as the life cycles and holders of cards and certificates.

Availability: A characteristic that describes how reliably the system, device, software or service is available for use.

Confidentiality: The notion that the information is only available to authorised persons, organisations or processes.

OCSP: Online Certificate Status Protocol, an online service that checks the status of a certificate

Personalisation software: Software used in registration points for the management of connections to the KoHa and Terhikki registers, the surface printing of certificate cards, and the recording of certificates on card microchips. The software is also used to create PIN codes and PUK unlocking codes.

PIN *(Personal identification number)*: The code used to verify the right to use the key pair of the certificate card. Healthcare certificate cards contain two PIN codes: one for authentication and encryption, and one for electronic signing.

Process: A series of transactions with a specific direction, purpose, effect or outcome, for example a certificate issuance process.

PUK (*Pin unblocking key*): A code used to unlock a blocked PIN code of a certificate card when the PIN has been entered incorrectly too many times in a row.

Registration authority (RA): In a public key infrastructure, a trusted party who performs RA duties, authorised and audited by the certification authority. The registration authority operates one or several registration points on behalf of the certification authority.

Registration point (RA point): A service point which verifies a certificate applicant's identity and the practice rights of regulated healthcare professionals and the employer information of other personnel. The registration point is responsible for the distribution of certificate cards, certificates and PIN/PUK codes to users in accordance with the certification practice statement and the certificate policy.

Certificate revocation list (CRL): The certificate revocation list is a list of certificates that have been revoked. A certificate is revoked upon request of the certificate holder or when the certificate holder's information recorded in the certificate has changed or the certificate card and PIN have been lost, and in the event of the certificate holder's death.

Revocation service: The certification authority's service that revokes service provider person's certificates on the basis of revocation requests.

Regulated healthcare professional: According to section 2(1) of the Act on Health Care Professionals (559/1994), a person who, on the basis of the Act, has been given the right to practise a profession (licensed professional) or the authorisation to practise a profession (authorised professional) and a person who, on the basis of the Act, is entitled to use the occupational title of a health care professional as laid down by Government decree (professional with a protected occupational title). For the purposes of this CPS, a regulated healthcare professional is also a student as referred to in section 2(3) of the Act on Health Care Professionals.

Non-regulated healthcare worker: Other, non-regulated personnel who work in a healthcare unit or perform its tasks.

Terhikki register: A national register of regulated healthcare professionals and their practice rights, maintained by Valvira on the basis of the Act on Health Care Professionals (559/1994).

Authentication: Verification of the authenticity of a system user (an individual, organisation, device or system) or a communication party. Common user authentication methods: 1) the user's knowledge of a unique piece of information such as a password, 2) the user's physical possession of a unique biometric characteristic such as a fingerprint, 3) the user's possession of a unique device such as a healthcare certificate card.

Identification: A procedure for identifying, for example, a user of an information system. Identification is typically done by verifying whether the presented user ID or other identifier is an approved identifier; for example, whether the user is on a list of authorised system users.

Security level: Security level refers to the level of security measures which are in place to safeguard against security incidents and attempts. For example, typical subjects of security level monitoring include information security incidents.

Key escrow: In the key escrow method, the secure storage of authentication and encryption keys is compulsory and the securely stored key can in some cases be used without the certificate holder's consent. The private keys of healthcare certificate cards are not held in escrow.

Certificate: In a service network that uses public key infrastructure, a dataset consisting of the public key and identification data of a party who operates in the network (e.g. a healthcare professional or service provider), created and signed by the certification authority via its private key. The authenticity of the certificate can be verified via the certification authority's public key (the CA certificate).

Certificate directory: The certificate directory is a public database used by the certification authority to store CA certificates, healthcare authentication and encryption certificates, and certificate revocation lists.

Certificate path: A chain of certificates required to facilitate secure communication between two parties that belong to different certificate administrations. It is implemented by having a common certification authority in place for the two certification authorities or by their mutual acceptance of each other's certificates.

Certification authority (CA): In public key infrastructure, a trusted party that produces key pairs for the system's users and creates, signs, distributes and revokes certificates.

Population Information System (PIS): A population register which contains basic information about Finnish citizens and foreign citizens residing permanently in Finland. The system also contains information about buildings, construction projects, apartment blocks, properties and operating premises. The Population Information System is maintained by the Digital and Population Data Services Agency and local register offices. In addition, updates are submitted by local parishes and hospitals. Registration of information is based on statutory notifications made by private individuals and public authorities.

2 Publication of data

2.1 Public directory

The certification authority is responsible for the maintenance of the certificate directory and the publication of information specified in section 2.2. The directory's data contents and structure are THPKI T3-compliant.

The directory administration is responsible for services related to the directories in accordance with the agreement and this CPS.

2.2 Data published by the certification authority

The certification authority ensures that certificate policies, certification practice statements, PKI disclosure statements and CA certificates are publicly available at www.fineid.fi. The directory service is a public Internet-based service which can be used to retrieve authentication and encryption certificates issued by the certification authority which are intended for publication in the public directory, and the certification authority's certificates and revocation lists. The directory service is available at ldap://ldap.fineid.fi.

2.3 Publication frequency

The certification authority publishes the certificate policy and the certification practice statement. The change management process is described in section 9.12.

Authentication certificates and certificate revocation lists are published in the certificate directory immediately after creation.

2.4 Access privileges

The availability of information published by the certification authority is not restricted.

3 Identification and authentication

The practices and procedures which are in place to identify and authenticate persons in the certificate order process are described in this section.

3.1 Naming of the certificate holder

3.1.1 Naming

The naming of a healthcare certificate holder in the authentication and encryption certificate and signature certificate is described in the specification: Digital and Population Data Services Agency's CA model = THPKI - T2: The Digital and Population Data Services Agency's CA model and the data contents of certificates in healthcare.

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 DPDSA's certification authority for organisation certificates is:

CN (Common name) = VRK CA for Qualified Certificates - G3

OU (Organizational unit) = Organisaatiovarmenteet

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Certificate holder naming policy for organisation certificates:

2.5.4.5 (Serial Number) = Unique identifier

SN (Surname) = Surname

G (Given name) = Given name

CN (Common name) = Surname Given name Unique identifier

C (Country) = FI

Optional fields:

O (Organization) = Name of the organization

OU (Organization Unit) = The organizational unit

T (Title) = Title

E (EmailAddress) = Email address

UPN (Universal Principal Name) = UPN name

3.1.2 Naming specification

Certificate holders are named using the given names and surnames of natural persons recorded in the Population Information System.

The set of attributes that forms the name record in the certificate is unique and identifies the certificate holder in question. The unique identifier is assigned by the certification authority. All non-regulated healthcare workers must use their own names.

3.1.3 Anonymity and pseudonyms

Anonymous certificates or certificates using a pseudonym (including stage/pen names) or nicknames will not be issued.

3.1.4 Contents of name fields

The contents of the name fields are specified in section 3.1.1.

3.1.5 Uniqueness of a name record

The name record specified in section 3.1.1 identifies the non-regulated healthcare worker's certificate holder. This personal identifier is unique.

3.1.6 Right to use brand names

—

3.2 Authentication of identity

3.2.1 Private key ownership authentication

The private keys of non-regulated healthcare workers are always created on the microchip of the certificate card. The certificate card containing the private keys is handed over to the healthcare worker once his/her identity has been reliably verified and the certificate has been registered and created.

3.2.2 Verification of the certificate holder's organisation

For non-regulated healthcare worker's certificates, verification of the organisation is required.

3.2.3 Personal identification

The applicant's identity is verified from a valid identity document issued by the police, which can be an identity card, a passport, or a driving licence issued after 1 October 1990. Other acceptable forms of identity are: a valid passport or identity card issued by an official government agency of an EEA member state, Switzerland or San Marino, a valid driving licence issued by an official government agency of an EEA member state after 1 October 1990, or a valid passport issued by an official government agency of another state. If the applicant does not hold any of these documents, the police will verify his/her identity by other methods. The identification information is stored in the certification authority's certificate order and management system (Vartti).

3.2.4 Information of the certificate applicant not verified by the certification authority

All personal information required for the non-regulated healthcare worker's certificate application is retrieved from the Population Information System and the employer information provided by the applicant's organisation.

3.2.5 Certification requirements

Non-regulated healthcare worker's certificates can only be applied for by persons who work in a healthcare unit or perform its tasks and who are not regulated healthcare professionals. The certificate must be revoked at the end of the employment relationship.

3.2.6 Prerequisites and requirements concerning cooperation between certification authorities

The prerequisites and requirements on cooperation between certification authorities are defined in the root CA policy.

3.3 Identification and authentication for certificate renewal

3.3.1 Identification and authentication for certificate renewal

The renewal of certificates adheres to the same procedures as when applying for the certificate for the first time.

3.3.2 Identification and authentication after revocation

The issuance of a new certificate adheres to the same procedures as when applying for the certificate for the first time.

3.4 Identification of the requester of revocation

Certificate revocation requests can be made by phone, in person at the registration point or by contacting the certification authority in writing.

When a revocation request is made by phone or in writing, the details of the requester and the certificate holder are recorded in the certificate order and management system (Vartti).

If the revocation request is made in person at the registration point, the card holder's identity is verified from a valid identity document issued by the police, which can be an identity card, a passport, or a driving licence issued after 1 October 1990. Other acceptable forms of identity are: a valid passport or identity card issued by an official government agency of an EEA member state, Switzerland or San Marino, a valid driving licence issued by an official government agency

of an EEA member state after 1 October 1990, or a valid passport issued by an official government agency of another state. If the applicant does not hold any of these documents, the police will verify his/her identity by other methods.

If the requester cannot be identified in a sufficiently reliable manner and there is a risk that the certificate could be misused, the certification authority will prioritise the revocation of the certificate.

4 Functional requirements for certificate life cycle management

The requirements on the actions of the certification authority, registration authority and non-regulated healthcare worker and the revocation of certificates are described in this section.

4.1 Applying for a certificate

Applications for non-regulated healthcare worker's certificates are made in person at the registration point.

The application information is stored in the certification authority's certificate order and management system.

The applicant is required to:

- prove his/her identity by a method specified in chapter 3
- present his/her personal information as described in section 3.2.3
- sign the application form.

The applicant will be notified of the method of delivery of the certificate card and the PIN code letter. The applicant is given the terms and conditions of use for the certificate, which are part of the certificate policy documents.

4.1.1 Who can apply for a certificate?

The certificate application can be made by a person who works in a healthcare unit or performs its tasks and who is not a regulated healthcare professional.

4.1.2 Certificate issuance process and responsibilities

The information of the issued certificate and the associated certificate card are registered using a system that ensures the integrity of the data.

Connections between the certification authority's information systems are encrypted. Persons who use the certificate order and management system are identified by management cards issued by the certification authority. The data contents of the certificate are based on the information provided in the application form.

After the registration authority and the applicant have checked and signed the certificate application, the registration authority submits the application to the certification authority who will issue the certificate.

Based on the application information, the certification authority sends to the applicant:

- a certificate card which contains the card holder's personal key pairs and certificates
- a PIN envelope which contains the personal PIN and PUK codes for the certificate card.

In addition, the certification authority sends the instructions for the use of the card.

4.2 Processing of the certificate application

The certificate application will be processed by the registration point without undue delay.

The registration authority enters the certificate order information in the certificate order and management system.

4.2.1 Implementation of identification and authentication

The registration authority verifies the certificate holder's identity in accordance with section 3 and ensures that he/she is employed at the healthcare unit in question.

The person's details are retrieved from the Population Information System. The application should state the applicant's preferred name of address to be used in the certificate. In addition, the registration authority completes the form with information regarding the applicant's employment relationship, information needed to produce and deliver the certificate, and the type of document used to identify the applicant.

4.2.2 Approval or rejection of the certificate application

The certificate application is approved by granting the certificate. If any of the prerequisites for issuing the certificate to the applicant are missing, the certificate is not issued and the application is rejected. The applicant is notified of the decision immediately, and he/she can appeal the decision in writing with the certification authority.

4.2.3 Certificate application processing time

Certificate applications are processed without undue delay during the opening hours of the registration point.

4.3 Granting of a certificate

4.3.1 The certification authority's duties in granting certificates

The certificate issuance process is initiated by a registration point officer. Access to the certificate system requires strong identification of the officer. The officer's actions are recorded in the log files of the certification authority's information systems.

The tasks related to certificate issuance are described in sections 4.1 and 4.2.

4.3.2 Notifying the applicant of certificate issuance

No separate notification is made when the non-regulated healthcare worker's certificate is issued.

4.4 Acceptance of the certificate

4.4.1 Certificate acceptance procedure by the certificate applicant

The certificate holder must check the accuracy of the information stored in the card and certificate. The certificate is then approved without further action by the certificate holder. If there are any problems, the certificate holder should contact the registration point or the support helpline.

4.4.2 Publication of the certificate by the certification authority

The certification authority publishes issued authentication and encryption certificates in a certificate directory located in a public network as described in section 2.1 Signature certificates are not published in a directory.

4.4.3 Notification of other parties of issued certificates

No separate notification is made when the non-regulated healthcare worker's certificate is issued.

4.5 Use of certificates and key pairs

4.5.1 Use of certificates and key pairs by the certificate holder

Non-regulated healthcare worker's certificates and the associated key pairs are intended for use only in social and health care information systems and associated services in Finland.

Non-regulated healthcare workers are required to adhere to this certification practice statement when applying for and using certificates.

A non-regulated healthcare worker is primarily responsible for any damages caused by him/her:

- by acting in breach of current acts, decrees or associated regulations or guidelines;
- by acting in breach of the certification practice statement;
- by acting in breach of the terms and conditions of use of a certificate accepted by him/her;
- by wilful or negligent misuse of the certificate.

The certificate holder must store and manage his/her certificates and key pairs and the associated codes and certificate card with due care. The certificate holder must take measures to prevent the loss of the certificate card and protect PINs against unauthorised disclosure or misuse.

The certificate card must not be left in a reader unattended or given to another person in any circumstances.

A non-regulated healthcare worker must notify the revocation service:

- of the loss or suspected misuse of his/her certificate card.

If the certificate card is damaged, the card holder must arrange for the certificates held on the card to be revoked and apply for a new card at the registration point. The card renewal procedure is the same as the procedure for applying for the card and the certificate for the first time.

PIN codes used to activate the keys must not be kept together with the certificate card. The certificate holder must change his/her PIN codes if there is reason to believe that they may have been disclosed to unauthorised parties.

If the PIN code is locked and the associated PUK unlocking code has been lost, the card holder must visit the registration point in order to obtain the unlocking code. When requesting the unlocking code, the card holder's identity is verified from a valid identity document issued by the police, which can be an identity card, a passport, or a driving licence issued after 1 October 1990. Other acceptable forms of identity are: a valid passport or identity card issued by an official government agency of an EEA member state, Switzerland or San Marino, a valid driving licence issued by an official government agency of an EEA member state after 1 October 1990, or a valid passport issued by an official government agency of another state. If the applicant does not hold any of these documents, the police will verify his/her identity by other methods. The registration point officer prints a new PIN code envelope which contains the unlocking code. For security reasons, the unlocking code must not be given over telephone or by letter.

4.5.2 Use of certificates and public keys by the trusting party

The trusting party is responsible for ensuring that the certificate is used only for the purpose specified in this CPS as regards its own information systems. The CPS reference contained in the certificate can be used to ascertain the appropriate use of the certificate.

The trusting party must ensure that its applications meet the requirements of this CPS.

The trusting party is responsible for duly verifying the certificate throughout the certificate path in accordance with the IETF RFC 5280 specification. If the certification authority and the trusting organisation have agreed on additional services related to the use of the certificate, the trusting party agrees to comply with the terms and conditions of said service.

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

The trusting party is responsible for verifying the validity of the certificate and for checking either the OCSP service or the current revocation list. The certificate should not be trusted before the trusting party has carried out the following revocation checks:

1. The trusting party must check the revocation path and its authenticity from the certification authority's digital signature.

2. The trusting party must check the validity period of the revocation list to ensure that the list is valid.

3. Certificates (the public key) can be stored locally in the trusting party's system, but the validity of the certificate must be verified before it is accepted.

If the current revocation list is not available due to a fault in the system or service, certificates under this CPS must not be accepted. If, however, the trusting party accepts the certificate, it does so at its own risk.

4.6 Re-certification of a public key

Non-regulated healthcare worker's certificates will not be issued on previously authenticated public keys.

4.7 Renewal of a certificate

4.7.1 Reasons for renewal

A non-regulated healthcare worker's certificate can be renewed when the previous certificate expires if the prerequisites for issuance specified in section 3.2.5 are still met.

In addition, a certificate can be renewed if the certificate holder's details change (insofar as it affects the data content of the certificate) or the card becomes damaged. In this case, the certificate holder must contact the registration point and apply for a new certificate card as described in section 4.

4.7.2 Certification renewal application

The certificate renewal application can be made by the certificate holder only.

4.7.3 Processing of certificate renewal requests

The renewal of certificates adheres to the same procedures as when applying for the certificate for the first time.

4.7.4 Notifying the applicant of card renewal

No separate notification is made when the non-regulated healthcare worker's certificate is renewed.

4.7.5 Acceptance procedure for renewed certificates from the point of view of the certificate holder

The renewed certificate is accepted as described in section 4.4.1.

4.7.6 Publication of a renewed certificate

Certificates are published as described in section 4.4.2.

4.7.7 Notifying third parties of certificate renewal

No separate notification is made when the non-regulated healthcare worker's certificate is renewed.

4.8 Amendment of a certificate

The data contents of a certificate cannot be altered after the certificate has been created. If the certificate holder's details change in a way that affects the data content of the certificate, he/she can apply for a new certificate and card as described in section 4.7

4.9 Revocation and suspension of a certificate

The certification authority maintains a 24/7 certificate revocation service. Details of revoked certificates are published in a certificate revocation list, which is signed by the CA and published in a public directory. Certificates cannot be temporarily suspended.

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

Digital signatures made before the certificate is revoked will not be rendered invalid by revocation.

4.9.1 Prerequisites for revoking a certificate

A certificate can be revoked:

- upon the certificate holder's request
- if the certificate holder leaves his/her position
- if the certificate card is lost, stolen or damaged
- if the PIN code and the certificate card are lost or stolen
- upon death of the certificate holder.

The certification authority may revoke a non-regulated healthcare worker's certificate, if the certificate is used in a way that violates this certification practice statement, the act on the electronic processing of client data in social and health care (159/2007) or the act on electronic prescriptions (61/2007) or associated regulations, requirements or guidelines.

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

4.9.2 Who can request revocation of a certificate

A certificate revocation request can be made by:

- by the non-regulated healthcare worker who holds the certificate, or his/her legal representative;
- the certification authority, if the conditions specified in section 4.9.1 are met.

4.9.3 The certificate revocation process

The certificate holder contacts the revocation service or the registration point to make a revocation request. The request can be made:

1. by calling the free revocation service at +358 800 162 622.
2. in person by visiting the registration point, or
3. by contacting the certification authority in writing.

The identity of the person making the request will be verified as described in section 3.4

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

- upon the death of the certificate holder.

When revoking the certificate, the following information is recorded:

- the certificate holder's personal information, as available
    - given names and surname

- unique identifier/registration number or ID number

- details of the person requesting revocation (if other than certificate holder)
- method of identifying the requester
- the date and time of the request
- the reason for revocation is recorded if the request is made by another person; the certificate holder does not need to a give a reason
- details of the person receiving the revocation request
- other additional information provided by the certificate holder
  - date of the loss of the certificate card, the date of death of the certificate holder, etc.
- details of the person executing the revocation
- the date of revocation.

If the person requesting the revocation of a certificate is not the certificate holder and the certificate holder has not contacted the certification authority or registration authority in connection with the revocation, the certificate holder will be notified of the revocation by letter. The certificate is revoked using the card management application, and the revocation data are held for 5 years.

4.9.4 The certificate holder's duty to request revocation

The certificate holder must request revocation of his/her certificate immediately by contacting the registration point or revocation service, if the conditions set out in section 4.9.1 are met.

4.9.5 Revocation request processing time

The revocation service and registration points process certificate revocation requests immediately.

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

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

The trusting party is responsible for verifying the validity data of the certificate. The certificate must not be trusted unless the trusting party has checked the validity of the certificate from a valid revocation list or OCSP service.

4.9.7 Publishing frequency of the revocation list

The updated revocation list is published every hour.

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

4.9.8 Maximum validity period of the revocation list

Each updated revocation list is valid for max. 8 hours. Each list specifies the end time of its validity.

4.9.9 Real-time certificate status check

Real-time certificate status check is not in use.

4.9.10 Requirements for real-time certificate status check

—

4.9.11 Other certificate status checking procedures

—

4.9.12 Revocation due to a compromised private key

If a certificate needs to be revoked due to a compromised private key, the regular revocation process applies.

4.9.13 Temporary suspension of a certificate

Certificates cannot be temporarily suspended.

4.9.14 Who can request suspension of a certificate

—

4.9.15 Procedures for certificate suspension

—

4.9.16 Restrictions on certificate suspension

—

4.10 Certificate status check

Certificate status checks are done using the revocation list. The trusting party must also verify that the validity period has not expired.

4.11 Certificate expiration

A certificate is valid for the general validity period, a period specific to the certificate in question, or until its revocation when the conditions for revocation are met.

4.12 Key escrow and key recovery

The authentication and encryption keys of non-regulated healthcare workers are not held in escrow. Therefore certificates cannot be used without the certificate holder's consent, and private keys cannot be recovered if the card is lost or damaged.

5 Physical, operational and HR security management

This section describes the physical security measures and operational and HR security measures required of the certification authority, registration authority and certificate holder. With regard to security requirements concerning the certification authority and registration authority, the VAHTI 5/2004 recommendation and, from 1 May 2011, the ISO/IEC 27002 standard apply.

5.1 Physical security management

The CA's private keys which are used to sign certificates and revocation lists are protected against physical breach.

The CA, registration points and the card manufacturer store their production equipment and backup copies in such a way as to prevent unauthorised access to stored data and prevent the alteration, forgery or destruction of the data. Backup copies are held both for data recovery and archiving purposes. In order to safeguard against accidents, backup copies are held separately from the certificate production system.

Detailed conditions on physical security management are set out in the certification practice statement. If necessary, the CA will separately agree on detailed physical security management procedures with its suppliers.

5.1.1 Location and structure of facilities

The registration point facilities are Class 1 (basic protection) facilities as per VAHTI 1/2002 recommendations.

Certificate production systems are located in Class 3 (special protection) ICT facilities as per VAHTI 1/2002 recommendations. ICT facilities are compartmentalised, and duplexed systems are located in different rooms which operate independently of each other.

5.1.2 Physical access control

Access to registration points is controlled by preventing unauthorised access with sufficient locking devices.

Certificate production systems are located in facilities which have 24h manned security, an electric locking system with event logging, and CCTV with recording facility. The facilities cannot be accessed without a personal access key, and all events are logged in the access control system.

5.1.3 Electricity supply and air-conditioning

The electricity supply and air-conditioning of registration points must be secured separately.

The certificate production systems are located in ICT rooms with backed-up electricity supply and air-conditioning. A contract must be in place for fuel supply in emergencies.

5.1.4 Water damage

Registration points are protected against water damage.

Certificate production systems are located in ICT rooms with raised floors, raised underfloor cable trunks, and a monitoring system with capability to detect water damage.

5.1.5 Fire

Registration points are protected against fire damage.

Certificate production systems are located in ICT rooms with automatic fire-extinguishing systems.

5.1.6 Storage of data devices

Data devices such as hard disks, diskettes, flash memory devices and optical memory devices which are used to store confidential information in registration points and certificate production must be handled and stored according to the same requirements as those concerning confidential paper documents. The confidentiality of a data item or a document is determined by the Act on the Openness of Government Activities (621/1999).

5.1.7 Disposal of data devices

The disposal of data devices used in registration points and certificate production which contain confidential information is handled by an appropriate contractor. Disposal certificates for destroyed devices are archived.

5.1.8 Backup over network

The certificate production system is backed up over an internal network of the certificate system.

5.2 Operational security management

The certification authority bears overall responsibility for the administrative and logistical functions related to the issuance of certificates and publication of revocation lists. Functions can be provided by another organisation contracted by the certification authority.

5.2.1 Roles related to tasks

The tasks of the CA and its contractors are allocated in such a way as to minimise the risk of accidental or wilful misuse of data or services. The certificate production tasks are role-based, and each user is given only the privileges pertaining to his role.

The certificate production roles are:

- system administrator
- system user
- registration authority and
- auditor.

In addition, under the act on the electronic processing of client data in social and health care (159/2007), the certification authority monitors and ensures the requisite data protection and data security of its service.

5.2.2 Number of persons required for certificate production tasks

Named organisations and persons acting on behalf of the certification authority.

At least two people are involved in the generation and administration of the CA's key pair. System-level changes in the certificate system require participation of at least two people. The identification and registration of a certificate holder requires one person.

5.2.3 Personal identification and authentication in different roles

The certification authority's employees who perform trusted duties referred to in section 5.2.1 each have a personal PIN-protected management card. The management cards are used to verify the user's access privileges to the certificate system or other related systems.

5.2.4 Roles requiring separation of duties

The registration authority cannot be the system administrator.

5.3 HR security management

5.3.1 Background, merits, experience and checks

System users' tasks are security-critical since they create and manage certificate and key data. A person who performs system user duties must be suitable for the role in question and understand the importance of security in his/her everyday tasks. Organisations authorised by the CA must ensure the trustworthiness of their personnel at all times.

Persons who perform the CA's duties must undergo a background check.

5.3.2 Background check procedure

Organisations authorised by the CA are responsible for the background checks and trustworthiness of their employees.

5.3.3 Training frequency and requirements

The CA and organisations who perform its duties each ensure sufficient training of their personnel. The CA organises training for registration point personnel.

5.3.4 Additional training frequency and requirements

—

5.3.5 Frequency and order of job rotation

—

5.3.6 Consequences for unauthorised activity

In addition to any legal consequences, if a person conducts unauthorised activity, his/her privileges to the CA's systems will be revoked permanently.

5.3.7 Requirements for subcontractor personnel

The personnel of organisations authorised by the CA must meet the requirements set out in section 5.3.1.

5.3.8 Documents given to personnel

Personnel who participate in certificate activity have access to this CPS as well as task-specific instructions.

5.4 Certificate system security monitoring

The security monitoring procedures described in this section apply to all hardware and system set-ups that are linked to the certificate ordering and issuance process.

5.4.1 Archived events

The CA will store the following data for security monitoring purposes:

1. Creations of system-level privileges and attempts to gain unauthorised access.
2. Procedure requests related to system updates and maintenance.
3. Installation of new software and software updates.
4. The time and date of each backup run and other descriptive data.
5. The certificate system's shutdowns, reboots and poweroffs.
6. The date and time of each hardware update.

With regard to certificates and the certificate system the CA keeps a record of:

1. All events related to the creation and revocation of certificates, including CA certificates.
2. All events related to the management of certificate signature keys.
3. All messages from the registration service, certificate distribution service and additional services (other than messages related to system management).
4. The log system reboots and shutdowns.
5. Changes to the log system configuration.

5.4.2 Frequency of log data analysis

Log data are analyses on a needs basis.

5.4.3 Log data storage period

Log data are held in accordance with the valid provisions on archiving.

5.4.4 Protection of log data

Only specifically authorised personnel have access to log data.

Log data are protected against alteration, loss, corruption and unauthorised use.

5.4.5 Log backups

Log data are backed up daily.

5.4.6 The log data collection system (internal/external)

The certification authority is responsible for the log data collection system.

5.4.7 Notifications on log events

The system user is not notified when log data are created.

Persons who are responsible for monitoring log data are notified separately of the following:

- attempts to gain unauthorised access;
- system shutdowns, reboots and poweroffs;
- software installations and updates.

5.4.8 Vulnerability assessment

The CA assesses and monitors the vulnerability of the certificate system and production environment based on risk analyses, and endeavours to minimise risks.

5.5 Archived materials

5.5.1 Archived documents, files and media

The certification authority archives the following information:

- certificate applications;
- signed approvals of certificate/other applications;
- certificate service agreements;
- issued certificates;
- cross-certification documents, including the grounds and decisions and operations carried out;
- certificate revocation requests;
- current and previous versions of certificate policies and certification practice statements;
- agreements concluded between the CA and registration points; and
- agreements related to the administration, use and management of the certificate system.
- Audit reports and records, including data security audits and system audits

5.5.2 Archive retention period

The provisions of the Archive Act (831/1994) are applied as the general law for archiving. In addition, the provisions on archiving as set out in the Act on Electronic Services and Communication in the Public Sector (13/2003) will apply.

5.5.3 Archive protection

Archive data can be accessed only by personnel who are specifically authorised to do so. Documents, files and other media are stored in a fireproof, access-controlled facility which can be accessed only by persons authorised by the CA.

Archive data are protected against alteration, loss, corruption and unauthorised use.

5.5.4 Archive backup procedures

No backup copies of archive data are made.

5.5.5 Archive file timestamps

Archived documents are dated. Timestamp service is currently not in use.

5.5.6 Archive collection system (internal/external)

The CA does not have a centralised archive collection system.

5.5.7 Availability and integrity of archive data

Only specifically authorised personnel have access to archive data. Archive data are protected against alteration, loss, corruption and unauthorised use.

5.6 CA key pair change

The CA creates a new key pair and CA certificate no later than five years and three months before the expiry of the previous CA certificate. The CA certificate is submitted to a public directory as described in chapter 2. In addition, the CA certificate is stored in a certificate card chip.

5.7 Incident precautions

5.7.1 Contingency plan for operational continuity in case of incidents

The CA has set in place a contingency and preparedness plan which facilitates uninterrupted operation and the recovery of the CA's systems in the event of an incident. Clear responsibilities, plans and procedural instructions are in place for incidents and exceptional situations.

5.7.2 Damage to the certificate system, software or data

The CA follows a continuity and recovery plan in exceptional circumstances.

5.7.3 Procedure if the private key of a certificate holder is compromised

Certificate holder's private keys are protected against physical breach and exposure of the keys. If the certificate holder's private key is compromised, the certificate in question will be revoked. The certificate holder will be issued with a new certificate card and new private keys.

5.7.4 Operational continuity after an incident

After an incident, the CA will endeavour to reinstate core system functions without delay.

5.8 Termination

5.8.1 End of the certification authority's operations

Termination refers to a situation where the CA's operation is permanently closed down. A situation in which the CA's services are transferred to another organisation or the CA issues a new CA certificate is not considered termination.

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

- All certificates that are valid and have been granted are revoked on one or several revocation lists whose validity period does not expire until the validity of the last revoked certificate has expired.
- The certification authority will revoke all authorisations of its contractual partners to carry out tasks pertaining to certificate life cycle management on behalf of the certification authority.
- The certification authority ensures that access to the certification authority's archives, as referred to in section 5.5.7, will be maintained also after the termination of the certification authority.
- Certificate revocation lists continue to be available in the specified manner until the end of their validity period.

5.8.2 Termination of the registration authority's operations

Termination of the registration authority's operations refers to a situation in which the authorisation granted by the certification authority to the registration authority to register non-regulated healthcare worker's certificates is permanently withdrawn.

Termination of the registration authority's operations is implemented in accordance with the agreement concluded between the registration authority and the certification authority.

6 Technical security management

This section describes the terms and conditions pertaining to the management of the public and private keys of the certification authority, registration authority and non-regulated healthcare workers, and the associated technical specifications.

Non-regulated healthcare workers' key pairs can be created by the certification authority or another organisation authorised by the CA. In any case, the CA will oversee compliance with the terms and conditions pertaining to the creation of key pairs and, for its part, ensure the functionality of key pairs.

6.1 Creation of key pairs and delivery to the certificate holder

6.1.1 Creation of key pairs

The CA key pair is created and stored in a hardware security module that conforms to the commonly accepted standards adopted by the European Commission and published in the Official Journal of the European Union, such as FIPS 140-1 or 140-2 level 3 approval.

The certificate holder's key pairs are created in the certificate card chip.

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

6.1.2 Delivery of a private key to certificate holder

The certificate key containing the private keys and the necessary PIN codes are delivered to the certificate holder by a method that prevents interception by unauthorised parties.

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

The certificate applicant's public key is transmitted between the CA's systems via secure data connections.

6.1.4 Delivery of the CA public key to trusting parties

The CA certificate containing the CA public key can be retrieved from the public directory or service provided by the CA. In addition, the CA certificate is stored on each individual healthcare certificate card.

6.1.5 Key length

CA keys are 4096-bit RSA keys.

Non-regulated healthcare workers' signature keys and authentication and encryption keys are min. 2048-bit RSA keys.

6.1.6 Creation and type of public keys

Key pairs are created using standardised, high-quality, commonly recognised and tested methods and hardware security modules.

6.1.7 Intended use of keys

Key uses

Non-regulated healthcare workers' key pairs are used for authenticating the certificate holder, data encryption, and advanced digital signing.

6.2 Protection of private keys and the management of the hardware security module

6.2.1 Applicable standards

The CA's private keys are stored in a hardware security module (HSM) which meets FIPS 140-1 or 140-2 level 3 requirements. The certification authority's private keys are protected against disclosure and unauthorised use.

The CA ensures that non-regulated healthcare workers' private keys which are stored on certificate cards are delivered to the person in accordance with this CPS.

The non-regulated healthcare worker's certificate card conforms to the applicable standards, such as ISO/IEC 7816, Javacard Platform 2.2.2 and GlobalPlat-form 2.1.1. The data content of the certificate card conforms to the THPKI T5 specification.

The card chip and operating system are security-certified. Accepted security certifications are: FIPS 140-1 or 140-2 level 3 or higher, Common Criteria EAL4+ and ISO/IEC 15408.

6.2.2 Private keys administered by multiple persons

CA's private keys require the presence of at least two people authorised to administer the keys.

The registration authority's and service provider person's private keys can only be administered and used by the key holder.

6.2.3 Private key escrow

No key escrow is in place for healthcare certificate cards.

6.2.4 Private key backup

A backup copy of the CA's private key exists.

The security features and storage of the backup copy conform to the security requirements pertaining to the original CA private key in all circumstances.

No copies of non-regulated healthcare workers' private keys are made or stored.

Non-regulated healthcare workers' private keys are not disclosed to unauthorised persons in any stage of the card life cycle and they are only ever stored on the healthcare certificate card.

6.2.5 Private key archiving

The CA's private keys are destroyed after expiry.

Non-regulated healthcare workers' private keys are not archived. The certification authority does not have access to the private keys of the certificate holders.

6.2.6 Processing of private keys in a hardware security module

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

6.2.7 Private key storage

The CA's private keys are stored in a HSM in encrypted form.

The certificate holder's private keys are stored in the chip of the certificate card in a way that prevents them from being read, altered, copied or moved.

6.2.8 Private key activation

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

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

In order for a microchip command to be executed on the private keys, the key must be activated using the correct PIN.

The PIN of the certificate card will be locked after five unsuccessful entries.

The certificate card can be unlocked. Unlocking requires input of the correct PUK code.

6.2.9 Preventing the use of private keys

The use of the CA's private keys is prevented by authorised personnel using management cards or by disconnecting power from the HSM where the CA's private keys are stored.

The use of private keys held on a certificate card is prevented by removing the card from the card reader.

6.2.10 Private key destruction

The CA's private keys can only be destroyed by the CA.

If the CA's operations are terminated, the CA's private keys and their copies are destroyed.

If a non-regulated healthcare worker wishes to destroy his/her private key, he/she must contact the revocation service and ensure that data stored in the certificate card microchip are destroyed, for example, by cutting the card and chip in half.

6.2.11 Security level classification for certificate cards and HSMs

Certificate cards and HSMs must meet the standards referred to in section 6.2.1 and the associated classes.

6.3 Other matters of key pair management

Data is collected on each individual process related to key creation. The data include the certificate card order details and the card numbers and certificates of manufactured certificate cards.

6.3.1 Public key archiving

The CA archives its certified public keys in accordance with section 5.5.

6.3.2 Validity period of certificates and keys

Non-regulated healthcare workers' certificates and key pairs are valid for max. 60 months. The validity period is calculated from the certificate's date of issuance. If necessary, certificates can be issued for a shorter term.

The CA's certificate and key pair are valid for 16 years from the date of key creation. The keys will not be used for any purpose outside of the validity period.

6.4 Activation data

6.4.1 Creation of activation data

Activation data i.e. the PIN code and PUK unlocking code are created in conjunction with certificate card management. PIN codes are based on random numbers. The PIN code protects the private keys held on the certificate card. The certificate holder can change the PIN to another number (min. 4 characters).

The PUK code which is needed to unlock a locked PIN is 8 characters long. The PUK code is stored in the CA's information system.

6.4.2 Protection of activation data

PIN codes are delivered to the certificate holder in a sealed PIN code envelope, and they are not known to anybody else. The certificate holder can change the PIN codes (min. 4 characters). PUK codes cannot be changed.

6.4.3 Other matters regarding activation data

—

6.5 Hardware security management

The CA's system security management includes, among others, strong identification, the traceability of actions and tasks related to the CA's private keys (down to the individual user) and the collection of log data. Hardware is located in protected facilities.

The security of the registration authority's system hardware is ensured by preventing unauthorised access.

6.5.1 Special requirements

VAHTI 5/2004 guidelines apply with regard to security requirements concerning system hardware.

6.5.2 Classification of hardware security

—

6.6 Life cycle security management

6.6.1 Management of systems development

The CA's systems are developed in development and test environments that are separate from the production system.

All updates of the CA's information systems require a functionality check carried out in the test environment before the update is installed. Updates are planned on a case-by-case basis and scheduled and communicated in advance. The plan includes a testing plan and the acceptance criteria.

In version upgrades, the functionality of the whole data processing chain of the system will be ascertained first. The implementation stage is designed in such a way as to facilitate fast recovery of the old version within a specified time.

6.6.2 Security management

With regard to systems security management, the VAHTI 5/2004 recommendation and, from 1 May 2011, the ISO/IEC 27002 standard apply. Security management is placed on:

- task allocation between persons in accordance with section 5.2;
- security monitoring;
- regular security audits;
- technical security solutions and methods; and
- an authorisation and acceptance procedure for application modifications.

6.6.3 Life cycle security classification

—

6.7 Network security management

The connections and networks of the CA's systems are strongly encrypted, protected and dedicated. The CA is responsible for network monitoring.

VAHTI 5/2004 guidelines apply with regard to security requirements for data connections.

6.8 Time stamp

Timestamp service is currently not in use.

7 Certificate and revocation list profiles

7.1 Certificate profile

The profile of the non-regulated healthcare worker's certificate is described in the DPDSA specification for the healthcare CA model = THPKI - T2: The Digital and Population Data Services Agency's CA model and the data contents of certificates in healthcare.

7.2 Revocation list profile

The profile of the non-regulated healthcare worker's certificate revocation list is described in the DPDSA specification for the healthcare CA model = THPKI - T2: The Digital and Population Data Services Agency's CA model and the data contents of certificates in healthcare.

7.3 Real-time revocation list check (OCSP)

An OCSP protocol is available.

8 Acceptance audit

The CA ensures that its certification activity conforms to this CPS and the certificate policy. 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.

The CA has the right to audit its technical suppliers in accordance with the audit procedure specified in the technical supply agreement in question. The audit is carried out at least once a year and at the start of each new contract period.

The audit is carried out to determine the technical supplier's compliance with the agreement, taking into account the requirements of information security management standards. Technical suppliers are generally assessed on the basis of the ISO 27001 standard and Traficom regulations.

The audit is carried out by Digital and Population Data Services Agency's Head of Information Management or an external auditor commissioned by DPDSA, who specialises in auditing technical vendors pertaining to certificate services. The audit is carried out considering the implementation of the eight areas of information security. Audited information security properties include confidentiality, integrity and availability.

The audit covers Traficom regulations on the information security requirements of certification authorities.

8.1 Implementation of acceptance audits

The certification authority's operation is audited at least once a year. The purpose of the audit is to ascertain the CA's compliance with the certificate policy and CPS. The CA is responsible for the implementation of the audit.

8.2 Auditor

The audit is carried out by a commonly recognised independent and reputable audit body that specialises in information systems and is located in Finland or another EEA member state.

8.3 The auditor's relationship with the audited party

The auditor and the audited party are unrelated and independent of each other.

8.4 Scope of the audit

In the audit, the certificate policy and the CPS are compared with the CA's activities across the board. The audit also includes the data security of the information systems used in connection with authentication and registration.

The CA's contractors and other suppliers are also included.

The audit results are presented in a statement.

8.5 Measures in the event of non-conformities

If non-conformities are found, the CA will take immediate action to rectify them.

8.6 Communicating the audit results

The audit findings regarding documents and operations are presented in the public statement which is part of the audit report. The complete audit report is available upon request to the CA's parties as applicable on the basis on agreements.

9 General terms and conditions

This section describes the duties and responsibilities of the CA, registration authority, certificate holder and other parties involved in the operation of the certificate system, and matters related to dispute resolution.

9.1 Fees and other compensations

Fees and other compensations are determined on the basis of section 22 of the act on the electronic processing of client data in social and health care (159/2007), section 25 of the act on electronic prescriptions (61/2007), the Act on Criteria for Charges Payable to the State (150/1992) and the Decree of the Ministry of Finance on the payment of Digital and Population Data Services Agency fees (873/2008).

9.1.1 Certificate issuance fee

—

9.1.2 Certificate usage fee

—

9.1.3 Certificate revocation fee or status query fee

—

9.1.4 Fees for other services such as Support Service

—

9.1.5 Refunds

Refunds are determined on the basis of agreements concluded between the parties of the certificate system.

9.2 Financial duties

In accordance with section 33 of the Act on Strong Electronic Identification and Trust Services (617/2009), the certification authority shall ensure that it has adequate financial resources for proper operation and for covering possible liabilities.

9.3 Confidentiality and data protection

The provisions of Finnish acts and decrees and good data management practices and principles must be adhered to with regard to confidentiality and data protection.

9.3.1 Private information

Private information can only be disclosed on the basis of Finnish law or regulations issued under the law or with the certificate holder's consent.

All private keys used or handled by the CA in activities under this CPS are kept secret.

Collected registers and log data will only be published if required under a Finnish act, decree or an associated regulation.

9.3.2 Public data

The public keys and revocation list of authentication and encryption certificates are public information and available in a public directory.

Identifiable information and other information related to a person or enterprise held in an issued certificate is public unless otherwise provided by agreements, Finnish acts, decrees or associated regulations.

9.3.3 Protection of private information

All parties of the certificate system must comply with Finnish acts, decrees and regulations on the protection of private information.

9.4 Privacy protection

The provisions of Finnish law on privacy protection shall apply.

9.4.1 Private information protection plan

The parties of the certificate system must ensure that a plan for the protection of private information is drawn up and implemented.

9.4.2 Private information handled in the CA's systems

The handling of private information in the CA's systems is subject to the provisions of Finnish law on the handling of private information and the protection of privacy.

9.4.3 Public information handled in the CA's systems

The handling of public information in the CA's systems is subject to the provisions of the Act on the Openness of Government Activities (621/1999).

9.4.4 Responsibility for the protection of private information

The CA ensures that private information handled in its systems is protected against unauthorised access.

9.4.5 Use or publication of private information with the certificate holder's consent

Confidentiality and data protection are described in section 9.3.

9.4.6 Disclosure of information to authorities

Information can be disclosed to authorities on the basis of acts, decrees and associated regulations.

9.4.7 Other circumstances in which information can be published

The CA will not disclose information in any other circumstances than those described above.

9.5 Intellectual property rights

All copyrights related to the CA's systems are determined by agreements concluded between the contract parties.

9.6 Parties' commitments

9.6.1 CA's commitments

The CA agrees to produce, maintain and develop healthcare certificate services in accordance with this CPS and the certificate policy.

9.6.2 Registration authority's commitments

The registration authority must, for its part, agree to produce, maintain and develop healthcare registration services in accordance with this CPS and the certificate policy.

9.6.3 The certificate holder's commitments

The certificate holder agrees to use the non-regulated healthcare worker's certificate and certificate card in accordance with this CPS, the certificate policy and the instructions issued to him/her.

9.6.4 Trusting parties' commitments

Trusting parties agree to ensure the compatibility of their healthcare systems with the non-regulated healthcare worker's certificates.

9.6.5 Other parties' commitments

—

9.7 Non-liability clause

The non-liability clauses included in the agreements concluded between the CA and its contract partner or in the CA's specific requirements concerning certificate holders and parties using the certificate system apply to the CA's partner, certificate holder and the party using the certificate system in the same way as non-liability clauses and limitations of liability set out in this CPS.

9.8 Limitations of liability

Digital and Population Data Services Agency's liability for damages related to the production of certificate services is determined according to the service agreement concluded with the certificate applicant. Digital and Population Data Services Agency is bound by the certification authority's liability for damages conformant to the Act on Strong Electronic Identification and Trust Services. Where applicable, the Tort Liability Act (412/1974) also applies.

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

The CA is not liable for damage caused by the disclosure of PIN codes, a PUK code and a certificate holder's private keys unless said disclosure is the direct result of Digital and Population Data Services Agency's direct actions.

The certification authority is not liable for indirect or consequential damage caused to the certificate holder. Neither is the certification authority liable for the indirect or consequential damage

incurred by a party trusting a certificate or by another contractual partner of the certificate holder.

The 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 card reader software used by the certificate holder or for the use of a certificate in contradiction to its intended use.

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

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

The certification authority is not liable for errors in the online service or applications intended for end users and based on a certificate or any resulting expenses. The responsibility of a certificate holder ends when they have reported the necessary data to the revocation service for revoking the certificate and when they have received a revocation notice from the official receiving the call. In order to terminate liability, the revocation request must be made immediately upon noticing the reason for the request.

The CA is not liable for any damages caused by the conduct of the certificate holder or the party using the certificate system in violation of the law, this CPS, the certificate policy or other instructions.

The CA is not liable for any indirect damages or damages caused by a force majeure.

The CA may specify other limitations of liability in agreements concerning the operation of the certificate system or requirements imposed on the certificate holder or a party using the certificate system.

9.9 Compensation for damages

Digital and Population Data Services Agency's liability for damages related to the production of certificate services is determined according to the service agreement concluded with the certificate applicant. Digital and Population Data Services Agency is bound by the certification authority's liability for damages conformant to the Act on Strong Electronic Identification and Trust Services. Where applicable, the Tort Liability Act (412/1974) also applies.

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

9.10 Validity and expiry

9.10.1 Validity of the CPS

This CPS will be valid until superseded by a new version of the certification practice statement in question.

9.10.2 Expiry of the CPS

This CPS does not have a predefined period of validity.

9.10.3 Effects of the expiry of the CPS

—

9.11 Communication between the parties of the certificate service

The CA and the parties involved in the certificate activity must notify each other of any changes concerning their activities. Changes are communicated in writing to all cooperation parties.

9.12 CPS change management

Changes to the CPS are at the discretion of the CA.

9.12.1 Amendment of the CPS

With the exception of corrections of layout or typographical errors or changes to contact information, no other changes to the approved CPS can be made without prior notice. All other changes must be communicated at least 14 days before the change takes effect.

9.12.2 Change notice

Changes concerning the CPS other than those specified in section 9.12.1 will be published by the CA on its website (www.fineid.fi) at least 30 days before the change takes effect.

9.12.3 Changes to the CPS identifier

The unique identifier of the CPS changes in accordance with section 1.2 every time the contents of the CPS change.

9.13 Settling of disputes

Any disputes related to the healthcare certificate service or this CPS shall be brought before the district court of the CA's domicile in Finland.

9.14 Governing law

The healthcare certificate service and this CPS are governed by Finnish law.

9.15 Jurisdiction

The provision of the healthcare certificate services shall be governed exclusively by Finnish law.

9.16 Other arrangements

9.16.1 Agreements

The certificate application and the general terms and conditions of use form the agreement concluded with the certificate holder. The terms and conditions of use are part of the certificate policy documents. The rights, responsibilities and duties of the certification authority and the certificate holder are specified in the certificate policy and CPS. By signing the certificate application, the non-regulated healthcare worker undertakes to observe the terms and conditions governing the use of the certificate. The certificate holder receives the current terms and conditions together with the certificate.

Further, upon signing, the non-regulated healthcare worker agrees to immediately notify the revocation service if his/her certificate card is lost or if there is a suspicion or possibility of its misuse.

The certification authority and its authorised registration authorities conclude an agreement which states each party's rights, responsibilities and duties.

The certification authority may conclude agreements with trusting parties and other parties. Each agreement must clearly state each party's rights, responsibilities and duties.

The certification authority concludes agreements with the certificate service supplier and component suppliers as necessary.

9.16.2 Transfer of rights

The parties of the healthcare certificate service shall not transfer any rights defined in the agreements to other parties without the certification authority's prior consent.

9.16.3 Partial invalidity clause

Any invalidity, illegality or unenforceability of an individual provision of this CPS will not affect the rest of the CPS.

9.16.4 Enforcement

In the event that the certification authority waives its entitlement to damages or other compensation in respect of a breach of contract, it shall not be construed as waiver of any other similar or future breach of contract.

9.16.5 Force majeure

The certification authority is not liable for any damages caused by natural disasters or other force majeure events.

9.17 Other terms and conditions

When interpreting and applying documents concerning the healthcare certificate services, this CPS, and the commitments agreed to between the parties of the certificate system, the Finnish-language versions of documents take precedence.