CERTIFICATION PRACTICE STATEMENT

for organisation certificates

OID: 1.2.246.517.1.10.23.1

ISO 9001

ISO/IEC 27001

Population Register Centre

DOCUMENT MANAGEMENT	
Owner	Jukka Santala
Author	Tuire Saaripuu
Checked by	
Approved by	

VERSION MANAGEMENT		
version no	action	date/author
v.1.0	Approved version 1.0., an eIDAS-compliant document	1.7.2016 TS
v.1.1	FICORA M72/2016 requirements	1 January 2017 TS
v. 1.2	Editorial changes, OCSP	14 September 2017

Contents

Definitions and abbreviations

Definitions

Activation data: A confidential data (PIN code) that is needed to activate private keys stored in a microchip and to use them in public key methods (e.g. electronic signatures).

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

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

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

Public key infrastructure: A data security infrastructure in which security services are provided by public key methods.

Public key method: A data security service, such as electronic identification, which is provided by using public and private keys, certificates and asymmetric encryption.

Card reader software: Card reader software is used in workstations as a so-called end-user application. It enables users to use their cards and certificates stored on it in various user and application environments such as public e-services, secure email and logging on to workstations.

Trusting party: A party that trusts the certificate data and uses the certificate for various data security services such as electronic identification of the certificate holder and authentication of digital signature.

Microchip: A technical platform that is used to store the certificate and private keys, integrated into a smart card, identity card, payment card or mobile terminal card.

Organisation certificate: A certificate pair issued by the Population Register Centre to a natural person; the data content of the certificate is determined by the Act on Strong Electronic Identification and Electronic Signatures.

PIN code: Activation data that activates a private key held on a microchip. PIN 1: the basic code for authentication and encryption. PIN 2: a signature code for digital signing.

PUK code: A code that is needed to unblock a locked PIN code.

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

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

Revocation list: A list of certificates revoked before the end of their validity period and the revocation dates, electronically signed and published by the certification authority. The revocation list specifies the publication dates of the current and next revocation list. Revoked certificates are added to the list.

Revocation service: A technical service provider that receives certificate revocation requests and submits them to the certificate system on behalf of the certification authority.

ID card: An organisation-specific ID card which contains the cardholder's organisation certificate in its technical component (microchip).

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

Certificate system: A technical data system used to create certificates and sign revocation lists.

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

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

Certificate register: A register conformant to the Act on Strong Electronic Identification and Electronic Signatures that a certification authority providing certificates to the public must maintain. Data must be held for at least 5 years after the expiry of the certificate.

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

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

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

Certification authority: An organisation that issues certificates, is responsible for their provision and draws up the certificate policy that describes its operation and the associated certification practice statement.

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

CA's private key: The private key used by the certification authority to sign its issued certificates and published revocation lists.

Certificate applicant: A person who requests an organisation certificate and is reliably identified in conjunction with the request.

Certificate holder: A person whose identity and public key are verified by the CA's digital signature and who holds the private keys linked with the certificate in question.

Certificate holder's signature certificate: The public key in the certificate verifies the digital signature made by the certificate holder with the corresponding private key. The signature code (PIN 2) is required for the signing.

Certificate holder's authentication and encryption certificate: A certificate used for electronic personal identification and data encryption. The certificate holder uses the private authentication and encryption key for electronic identification and decryption of encrypted data or messages. The use of the key requires a basic PIN code (PIN 1).

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

Private key: The private component of a key pair used in asymmetric encryption in public key methods. The private keys of the certificate holder are stored on a microchip to protect them from unauthorised usage.

Abbreviations

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module
EPI	Electronic Personal Identification
HTTP	Hypertext Transport Protocol
ISO 27001	ISO/IEC 27001
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PDS	PKI Disclosure Statement
PIN	Personal Identification Number, PIN
PKI	Public Key Infrastructure
PUK	PIN Unblocking Key, PUK code
RSA	Rivest, Shamir, Adleman, a public key algorithm, asymmetric algorithm
PRC	Population Register Centre

1 Introduction

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

This CPS applies to the PRC's organisation certificate stored on an ID card.

The organisation certificate is a certificate under the Act on Strong Electronic Identification and Electronic Signatures.

1.1 General points

PRC offers highly secure digital signature and authentication certificates and associated services for the public and private sectors. 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 signature certificates and identification by strong electronic identification devices enable citizens to access public services online securely and flexibly anytime, anywhere. Signature certificate and strong electronic identification service providers are supervised by the Finnish Communications Regulatory Authority (FICORA).

A certificate is an electronic certificate that links the signature authentication data to the signatory and identifies the signatory. The certificate data are signed electronically by the CA's private key. Certificates under this certificate practice statement are based on a public key infrastructure and public key methods. The data contents of certificates under this CPS are determined by the Act on Strong Electronic Identification and Electronic Signatures.

This document specifies the procedure requirements that apply to certification authorities that grant signature certificates and to Population Register Centre, 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 Population Register Centre 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 Population Register Centre.

The Population Register Centre, which acts as the certification authority, uses an identifier to identify the certificate holder. This identifier is also a part of the data content of the certificate. The identifier is a technical data item created separately for e-service access, and it does not contain any personal information.

An organisation certificate can be stored on various ID cards.

Both the certificate policy and the certification practice statement of PRC have a unique object identifier (OID).

The certification authority's activities include the provision of certification, directory and revocation services, registration, and ID card creation and identification. These activities are described in Chapter 1.3.

PRC draws up a separate certificate policy for each type of certificate issued by it, and a separate certification practice statement for each technical platform. The certificate policy contains a general description of the practices, terms and conditions, responsibility allocation and other matters related to certificate usage for each type of certificate. The certification practice statement contains a detailed description of the applicable practices.

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. This document describes the procedural requirements concerning the activities and administrative practices of certification authorities that issue identification and signature certificates under the Regulation. The use of a secure signature creation device is described in the procedural requirements specified in this document.

Provisions on trust services are set out in the Act on Strong Electronic Identification and Electronic Signatures (617/2009)

According to the Act on Strong Electronic Identification and Electronic Signatures, the PRC acts as an identification service provider when it offers certificate-based identification devices to the public.

In addition, as of 1 December 2010, PRC 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 Population Information System and the Certificate Services of the Population Register Centre (661/2009).

This certification practice statement describing the issuing of an organisation certificate has been registered by Population Register Centre.

The organisation 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 set out in the Regulation. The correctness of the certificate applicant's identity is guaranteed by Population Register Centre.

This certification practice statement describes the issuing and production of a signature certificate for digital signatures conformant to the Act on Strong Electronic Identification and Electronic Signatures 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 Electronic Signatures, included in the organisation certificate, conforming to the requirements of the production environment of the certificate.

1.2 Identifiers

The certification authority draws up a certificate policy for each issued certificate type and a certification practice statement for each technical platform the certificate can be used on.

The title of this certification practice statement is the Certification Practice Statement for PRC's Organisation Certificate, OID 1.2.246.517.1.10.23.1.

This certification practice statement refers to the Certification Policy for PRC's Organisation Certificates, OID 1.2.246.517.1.10.23.

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.

Population Register Centre 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], clause 4.3.5. 3) 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 28 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.

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

1.3 Certification authority and applications of certificates

The certification authority provides certificate services according to the terms and conditions specified in this certification practice statement and guarantees their functioning to the certificate holder in accordance with Chapter 2.2.1 on the responsibilities of the certification authority. The certification authority is responsible for the functioning of the certificate system as a whole, including on behalf of any registration authorities and technical suppliers it may use. This certification practice statement has been registered by the Population Register Centre. PRC is a public authority which administers a personal information register and, under the Act on the Population Information System and the Certificate Services of the Population Registration Centre (661/2009), is responsible for providing certified electronic services in addition to its other tasks. The PRC Certificate Service is comprised of the following functions:

1.3.1 Certification authority

The certification authority's task is to:

- provide certificate and directory services in accordance with its certificate policy and certification practice statement, and certification revocation services
- identify certificate applicants
- ensure the accuracy of the data content of certificates
- revoke certificates and publish certificate revocation lists
- adhere to high data security standards and good data processing practices when processing the personal information of certificate holders
- create client IDs for the purpose of personal identification
- provide a card order and management system for the registration of organisation cards.

1.3.2 Registration authority

Organisation certificates are registered in accordance with the Act on Strong Electronic Identification and Electronic Signatures. Organisation certificates located on organisation-specific ID cards are registered by PRC's partner with whom PRC has concluded a registration agreement.

- The registration authority acts on behalf of and at the responsibility of the certification authority.
- The registration authority shall comply with the certification authority's certificate policy and certification practice statement.
- The registration authority identifies certificate applicants in accordance with the certification practice statement.
- Certificates are created based on personal identification details related to the certificate application, which are provided by the registration point.
- The registration authority adheres to the principles of good personal data processing.
- PRC oversees that the client organisation adheres to the terms and conditions of the registration agreement and the relevant provisions of the Act on Strong Electronic Identification and Electronic Signatures.
- The registration authority uses the order and management system provided by the certification authority to register and order organisation cards.

1.3.3 Manufacturer and identifier of the ID card or microchip

- With regard to certificates, the associated key pairs and activation data, the manufacturer and identifier act on behalf of the certification authority, at its responsibility and in accordance with the agreement.
- The manufacturer and identifier shall comply with the certification authority's certificate policy and certification practice statement.

- Smart cards and microchips are uniquely identified in accordance with data provided by the registration authority.

1.3.4 Revocation service

The certificate revocation service revokes a certificate when the certificate holder wishes to revoke it before its stipulated expiry date. Revoked certificates are added to the revocation list.

1.3.5 Directory service

The directory service is a public Internet-based service which can be used to retrieve all organisation certificates issued by the certification authority which are intended for publication in the public directory, and the certification authority's certificates and revocation list. The directory service is available at ldap://ldap.fineid.fi.

1.3.6 Certificate holder

Organisation certificates under this certificate policy can be issued to persons identified in accordance with the Act on Strong Electronic Identification and Electronic Signatures.

The certificate holder must comply with the certification authority's certificate policy and certification practice statement.

1.3.7 The trusting party

The trusting party is a natural person or an organisation that trusts the certificate information and uses the certificate for authentication, encryption and electronic signing. The trusting party must verify that the certificate is valid and not on a revocation list.

1.3.8 Certificate usage

PRC adheres to this certification practice statement when issuing organisation certificates. Certificate holders and trusting parties must comply with this certificate policy.

Organisation certificates issued under this certification practice statement can be used for personal authentication, encryption and electronic signing. The certificate can be used without limitation according to its purpose in administrative applications and services and those provided by private organisations.

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

1.4 Contact details

1.4.1 Organisation responsible for administering the certification practice statement

This certification practice statement has been registered by the Population Register Centre (PRC). PRC is responsible for the administration and updating of this certification practice statement.

1.4.2 Contact person

Questions regarding this certification practice statement should be addressed to :

Population Register Centre (PRC)
P.O. Box 123 (Lintulahdenkuja 4)
00531 Helsinki
Business ID: 0245437-2

vaestorekisterikes-kus@vrk.fi
Tel. +358 295 535 001
Fax. +358 9 876 4369

Questions regarding the certificate policy are handled by the Certificate Services unit of PRC. Registration manager Tuire Saaripuu is responsible for communications related to these documents.

2 General terms and conditions

This certification practice statement is effective as of 14 September 2017.

2.1 Obligations

2.1.1 Certification authority's obligations

- The PRC is a statutory certification authority.
- The client organisation is for its part responsible for revoking certificates in accordance with the agreement made between PRC and the client organisation.
- The client organisation shall verify the accuracy of information about end users in accordance with the agreement made between PRC and the client organisation.
- The certification authority shall act in accordance with current legislation.
- The certification authority shall perform its duties duly and reliably.
- The certification authority has the necessary technical ability, financial resources and ability to cover its liability for damages.
- The certification authority is responsible for all areas of the certification activity, including the reliability and functioning of services and products produced by any technical suppliers or persons who assist the certification authority, such as registration authorities and card manufacturers.

- The certification authority draws up and maintains a certificate policy which describes at a general level the procedures for the issuance, maintenance and management of organisation certificates, the terms and conditions, the allocation of responsibilities, and other matters related to the use of organisation certificates.
- The certification authority draws up and maintains certification practice statements which describe how the certification authority applies its certificate policy.
- The certification authority complies with its certificate policy and certification practice statement.
- The certification authority makes the certificate policy and the certification practice statement publicly available.
- The certification authority shall employ sufficient staff with the expertise, experience and competence required for producing certificate services.
- The certification authority shall use reliable systems and products protected against unauthorised use.
- The certification authority shall keep information regarding the certificate and certificate activities publicly available, based on which the operations and reliability of the certification authority can be assessed.
- The certification authority ensures the confidentiality of signature creation data.
- The certification authority will not store or copy any signature creation data provided to a signatory.

2.1.2 The registration authority's obligations

- The registration authority shall comply with the certificate policy and the certification practice statement in its registration activities.
- The registration authority identifies the certificate applicant personally and reliably in a way described in the certification practice statement and so that the applicant's identity and other information pertaining to the applicant's person needed in the granting of the certificate will carefully be inspected.
- The registration authority shall see to the careful handling and confidentiality of personal data.
- The registration authority shall provide the certificate applicant with data of the terms of use of the certificate.
- The registration authority shall adhere to registration procedures agreed upon with the certificate authority.

2.1.3 Certificate holder's obligations

- The purpose of the certificate is specified in the certificate policy and certification practice statement of each certificate type and in the certificate holder's instructions. The certificate may only be used in accordance with its intended use for digital signing, authentication or encryption.
- The holder of an organisation certificate sees to it that the data stated when applying for organisation certificates are correct.
- The holder of an organisation certificate is liable for the use of the organisation certificate, legal actions taken with it and their financial consequences. With respect to an organisation certificate, the provisions of the Regulation and the Act on Strong Electronic Identification and Electronic Signatures apply.
- The holder of an organisation certificate shall store its private keys contained on a microchip and the PIN code required for using them separately from each other and aim to prevent the loss, access by third parties, alteration or unauthorised use of the private keys. Transferring the microchip or disclosing the PIN code to a third party, for example by lending, releases the certificate authority and the party trusting the organisation certificate from any liability arising out of the use of the microchip.
- The organisation certificate shall be handled and protected with the same care as other corresponding microchips, cards or documents, such as credit cards, driving licence or passport. Personal PIN codes must be stored physically in a different location than the microchip containing the organisation certificate and private keys.
- The loss or suspected misuse of the microchip and card must be reported without delay to the certification authority by calling the free-of-charge revoking service at +358 800 162 622. Deaf and hard-of-hearing customers can contact the textphone service at +358 100 2288.

2.1.4 Obligations of the party trusting a certificate

It is the obligation of the party trusting a certificate to ensure that the certificate is used according to its intended use. The intended use of a signature certificate is electronic signing. The intended use of an authentication and encryption certificate is the authentication of a person and encryption of data.

A party trusting the certificate must adhere to the certificate policy and certification practice statement.

A party trusting an organisation certificate may bona fide trust an organisation certificate after verifying that *the organisation certificate is valid and is not contained on a revocation list.* A party trusting an organisation certificate shall check the certificates on the revocation list. The certification authority provides an online certificate status check service that implements OCSP. In order to reliably verify the validity of an organisation certificate, the trusting party must comply with the following procedure for revocation list checks.

If a party trusting an organisation certificate copies the revocation list from a directory, it must verify the genuineness of the revocation list by checking the digital signature of the revocation list's certification authority. In addition, the validity period of the revocation list must be checked.

If the most recent revocation list cannot be obtained from the directory because of hardware or directory service malfunction, the organisation certificate must not be accepted if the validity period of the last obtained revocation list has expired. All approvals of an organisation certificate after the validity period take place at the risk of the party trusting the organisation certificate.

2.1.5 Obligations pertaining to the publishing of a certificate

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

2.2 Liabilities

2.2.1 Certification authority's liabilities

Population Register Centre as a certification authority is liable for the safety of the entire certificate system. The certification authority is liable for services it has commissioned as if for its own.

Population Register Centre is responsible for the organisation certificate having been created with adherence to the procedures prescribed in the Act on Strong Electronic Identification and Electronic Signatures, the Act on Electronic Services and Communication in the Public Sector, the certificate policy and the certification practice statement and according to the data provided by the applicant of the certificate, and for compliance with the certification authority's liability for damages as provided by law. Population Register Centre is liable only for the data it has stored in the certificate.

Population Register Centre is liable for the usability of the organisation certificate, when used appropriately, throughout its validity period, unless it has been placed on a revocation list. The organisation certificate has been given to a person identified in a manner required for organisation certificates. The certificate holder has been given instructions pertaining to the use of the organisation certificate prior to the signing of the agreement.

When signing an organisation certificate with its private key, the certification authority assures it has checked the personal data in the organisation certificate according to the policies described in the certificate policy and the certification practice statement.

The certification authority is responsible for including the right person's organisation certificate on the revocation list and that it appears on the revocation list in the time specified in this certificate policy.

2.2.2 Registration authority's liabilities

The registration authority of an organisation certificate is a registration point that registers the certificate applicant for Population Register Centre, which acts as the certification authority, on the basis of an agreement concluded for this purpose. The registration authority is responsible

for registrations performed by it. Registrations are subject to the requirements set out in the Act on Strong Electronic Identification and Electronic Signatures.

2.2.3 Certificate holder's liabilities

The holder of a certificate is liable for the use of the organisation certificate, legal actions taken with it and their financial consequences.

Leaving a card containing a microchip in a reader may enable the abuse of the organisation certificate. When terminating a terminal session, it is the responsibility of the certificate holder to remove the microchip containing the organisation certificate from the reader device and close the applications used appropriately or otherwise closing the technical connection needed for the use of the certificate.

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.

2.2.4 Liabilities of a party trusting a certificate

A party trusting a certificate cannot bona fide trust it and the correctness of the digital signature if the validity of the organisation certificate has not been checked on the revocation list. The certification authority provides an online certificate status check service that implements OCSP. Accepting an organisation certificate in the above cases releases Population Register Centre of liability. A party trusting an organisation certificate shall verify that the certificate granted corresponds to its intended use in the legal action in which it is used.

2.2.5 Limitations of liability

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

Population Register Centre is not liable for damage caused by the disclosure of PIN codes, a PUKD code and a certificate holder's private keys unless said disclosure is the direct result of Population Register Centre's direct actions.

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

Population Register Centre is not liable for indirect or consequential damage caused to the certificate holder. Neither is Population Register Centre liable for the indirect or consequential damage incurred by a party trusting an organisation certificate or by another contractual partner of the certificate holder.

Population Register Centre 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.

2.3 Financial liability

2.3.1 Certification authority

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

2.3.2 Other parties

A party trusting an organisation certificate may trust the correctness of the digital signature of an organisation certificate if they have verified that the organisation certificate has not been included in a revocation list, the validity of the certificate has not expired and the party has no other justifiable reason to doubt the correctness of the use of the certificate. The certification authority provides an online certificate status check service that implements OCSP.

The certification authority is responsible for the organisation certificate in accordance with the certification authority's commitments in this certificate policy and the certification practice statement on organisation certificates.

2.3.3 Certification authority's financial administration

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

2.4 Interpretation and implementation

2.4.1 Applicable legislation

A signature certificate granted in conformance with this certificate policy meets the requirements of the Regulation.

Provisions on digital signatures are set out in the Act on Strong Electronic Identification and Electronic Signatures (617/2009)

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

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

In accordance with the Act on Electronic Services and Communication in the Public Sector, signature certificates can be used in all communication with public administration.

Population Register Centre conforms to the principles of good personal data processing set forth in the Personal Data Act (523/1999) and to the good information management practices of the Act on the Openness of Government Activities (621/1999). Population Register Centre also secures information security with continuous training. Population Register Centre has also prepared policy rules for information services and certificate services.

Population Register Centre procures the duties pertaining to registration and personal identification under a separate, private-law contract pertaining to registration measures. Population Register Centre may obtain a service, for example, by adhering to the regulations set forth in the act on the government's joint services (223/2007).

The position of Population Register Centre is prescribed in the register administration act (166/1996) and decree (248/1996).

In Finland, signature certificate authorities are supervised by the Finnish Communications Regulatory Authority.

Population Register Centre is responsible for the organisation certificates having been created with adherence to the procedures prescribed in the Act on Strong Electronic Identification and Electronic Signatures, the Act on Electronic Services and Communication in the Public Sector and the certificate policy and according to the data provided by the applicant of the certificate.

The certificate services of Population Register Centre are supervised by Finnish Communications Regulatory Authority (FICORA), a body conformant to the Act on Strong Electronic Identification and Electronic Signatures, which issues regulations and recommendations on certification

activities. For that reason, PRC does not participate in voluntary accreditation systems. With respect to the processing of personal data, Population Register Centre conforms to the Personal Data Act. Population Register Centre works in constant collaboration with the Office of the Data Protection Ombudsman with respect to the processing of personal data.

Applicable legislation is adhered to in settling appeals and disputes, in administrative supervision and implementation of law. In the provision of organisation certificates, the Act on Strong Electronic Identification and Electronic Signatures and the supervision and appeals procedure described therein must, in particular, be taken into account.

2.4.2 Settling of disputes

When granting organisation certificates, Population Register Centre is responsible for the certificates meeting the requirements set in this certification practice statement and the certificate policy for organisation certificates. Any disputes shall be settled according to Finnish law.

2.5 Fees

This section specifies the fees related to the use of an organisation certificate.

2.5.1 Granting and renewing an organisation certificate

Organisation certificates are applied for according to the description of the certification practice statement.

The price of acquiring an ID card is determined according to the then-valid Decree of the Ministry of Finance on the payment of Population Register Centre fees

The prices of organisation certificates stored on other microchips are determined according to PRC's current list prices for commercial services.

2.5.2 Fees related to the use of an organisation certificate

The certification authority does not separately charge the certificate holder for the use of the certificates, the revocation service or a public directory. Individual online service providers may charge for the use of their services. The use of a certificate does not require a specific announcement or permit from the certification authority.

2.5.3 Fees related to the revocation of an organisation certificate

Reporting an organisation certificate to a revocation list is free of charge. Retrieving revocation lists from the directory and checking the validity of organisation certificates against the revocation list are also free of charge.

2.5.4 Other fees

The use of advisory services is subject to a separate fee according to the then-valid price list.

If the service provider wishes to arrange for information maintenance service between the unique identifier of the organisation certificates and the identifiers of its own background system or between other updated data, the service provider may apply for information disclosure

permission in the information service from Population Register Centre. This service will be priced according to the then-valid Act on Criteria for Charges Payable to the State and the Decree of the Ministry of Finance on the payment of Population Register Centre fees.

The terms of use of an organisation certificate are given to the holder of the organisation certificate when receiving the organisation certificate.

2.6 Publishing and availability of data

2.6.1 Publishing of the certification authority's data

The certification authority publishes all of the certification authority's organisation certificates and revocation lists in a non-chargeable, publicly available, public directory. The certification authority publishes the certificate policy, the certification practice statements, the PKI disclosure statement (PDS) and other public documents pertaining to the production of certificate services on its website.

2.6.2 Publication frequency

Each organisation certificate is published in the public directory immediately upon its creation and remains in said directory for as long as it remains valid. The certification authority publishes a revocation list that is valid for eight hours from its publication. This revocation list is updated once per hour with a new one.

2.6.3 Availability of data

Directory and revocation list data are publicly available. The FINEID specifications published by the certification authority are available on the certification authority's website. In addition, the certificate policies and certification practice statements are available on the certification authority's website.

2.6.4 Repositories

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

2.7 Information security audit

Finnish Communications Regulatory Authority (FICORA) may audit the operation of a certification authority under the prerequisites set forth in the Act on Strong Electronic Identification and Electronic Signatures.

2.7.1 Audit frequency

Population Register Centre audits the facilities, devices and operations of its technical suppliers in an appropriate fashion. The audit is carried out at least once a year and at the start of each

new contract period. In its audit procedure, the Population Register Centre adheres to the practices set out in the ISO/IEC 27001 information security management standard.

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/IEC 27001 standard and FICORA regulations.

2.7.2 Auditor

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

2.7.3 Audit objects and scope

The objects of the audit are determined by the Act on Strong Electronic Identification and Electronic Signatures or, if Population Register Centre is carrying out the audit, the information security standard ISO/IEC 27001 or the technical terms of delivery.

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

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

The audit compares the policy, certification practice statement and application instructions to the operation of the entire certificate organisation and system. Population Register Centre ensures that the application instructions are consistent with the certificate policy.

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

Revocation service:

- communications security
- human resources security
- physical security

Certificate production:

- task allocation and personal tasks – human resources security
- physical security
- security related to the CA's keys
- the certificate production system and the backup system

- communications security

Card production:

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

Directory service:

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

HelpDesk operation:

- communications security
- personnel's competence and training
- processes for auxiliary functions

2.7.4 Measures resulting from deviations

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

2.7.5 Communicating the result of an audit

The results of an audit are communicated according to the law, the information security standard ISO/IEC 27001, Population Register Centre's information security policy and the valid terms of delivery. A detailed, fixed-form audit result intended for internal use is confidential and will not be disclosed to the public. Fixed-form reports are prepared separately for use outside of the organisation.

The PRC communicates the audit results to FICORA in accordance with the Act on Strong Electronic Identification and Electronic Services and FICORA's regulations and recommendations.

2.8 Publication of data

2.8.1 Data published by the certification authority

The data in the certificate system are confidential unless they are based on the regulations on information disclosure set forth in the Personal Data Act, the Act on the Openness of Government Activities, the Act on the Population Information System and the Certificate Services of the Population Register Centre (661/2009) the Act on Strong Electronic Identification and Electronic Signatures or for purposes set forth in the certificate policy or certification practice statement.

2.8.2 Public data

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

2.8.3 Data related to the expiry or revocation of an organisation certificate

The start and expiration date/time of the validity period of an organisation certificate are stored in the certificate. Certificates revoked during their validity period are published on a revocation list available to all.

2.8.4 Data disclosed to authorities

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

2.8.5 Other data

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

2.8.6 Disclosure of data on the request of the certificate holder

The holder of a certificate has the right to receive information pertaining to him/her, for example personal data, in accordance with the applicable legislation.

2.8.7 Other principles concerning disclosure of information

It is material for the reliability of the certification authority that Population Register Centre take all measures to see to the secrecy of confidential material it obtains in connection with the certificate activities and to the good administration of data unless otherwise required by legislation pertaining to the right of authorities to obtain information on the operation of the certificate system.

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

2.9 Intellectual property rights

Population Register Centre owns all data pertaining to the certificates and documentation in accordance with the technical terms of delivery. Population Register Centre has full ownership and utilisation rights to this certification practice statement and organisation certificate policy.

3 Identification of certificate applicant

3.1 Registration

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

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

The application document and terms and conditions of use clearly state that the applicant for organisation certificate, with his/her signature, confirms the correctness of the information provided and approves the creation of the organisation certificate and its publication in a public directory. At the same time, the applicant accepts the rules and terms pertaining to the use of the organisation certificate and sees to the storage of organisation certificates and PIN codes and the reporting of any misuse or lost cards.

Agreements have been concluded between the certification authority and registration authority, card manufacturer and other vendors that produce parts of the certificate services, indisputably specifying the rights, liabilities and obligations of all parties.

The organisation certificate applicant is responsible for the correctness of all material data that the applicant has given the certification authority or registration authority. The organisation certificate holder must use the organisation certificate only for its intended uses.

When a certification authority grants an organisation certificate, it also approves the application for certificate.

It is the responsibility of the organisation certificate holder to prevent the use of private keys and the related PIN codes belonging to him/her in a way contradictory to the terms of use and to take care of them as set forth in the terms of use.

The certificate holder must immediately notify the revocation service if he/she suspects that his/her organisation certificate may have been used in breach of the terms and conditions.

3.1.1 Naming policies

The PRC's root certificate authority is:
CN (Common name) = PRC Gov. Root CA
OU (Organizational unit) = Certificate Services
OU (Organizational unit) = Certification Authority Services
O (Organization) = Population Register Centre CA
S (State) = Finland
C (Country) = FI

The PRC's certification authority for organisation certificates is:
CN (Common name) = PRC CA for Qualified Certificates G2
OU (Organizational unit) = Organisation certificates

O (Organization) = Population Register Centre CA
S (State) = Finland
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 Client ID
C (Country) = FI

Optional fields:
O (Organization) = Name of the organization
OU (OrganizationalUnit) = The organizational unit
T (Title) = Title
E (EmailAddress) = Email address
UPN (Universal Principal Name) = The UPN name

The certification authority's public key is part of the certification authority's certificate. The certification authority's certificate is available in a public directory. If an organisation certificate is located on an ID card, the certification authority's certificate is also placed on the microchip of the ID card.

Data pertaining to the certificate holder unambiguously identify the certificate holder. The certification authority will determine the official identity of the certificate holder, if necessary.

3.1.2 Delivery of private keys to the certificate holder

Private keys pertaining to an organisation certificate, created on a microchip or other secure environment, are delivered to the certificate holder in connection with delivery. No copy of private signature keys created on a microchip exists or can be made afterwards. Key recovery can be performed on the authentication and encryption certificate in accordance with the agreement made between PRC and the certificate client organisation.

An ID card that contains an organisation certificate must be collected by the certificate holder in person by visiting the CA's registration authority. The organisation certificate holder must prove his or her identity in accordance with the procedure used in the application stage. The method of identification is recorded in the receipt note, which is signed by the customer and the registration authority's representative who hands over the ID card.

The basic ID and signing ID codes needed for the use of the card are sent by mail by the card manufacturer to the person specified in the application to the address given in the application.

3.2 Renewal of key pair

The public keys in organisation certificates and the private keys in the microchip cannot be renewed. The creation of new key pairs requires a new organisation certificate.

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

3.3 Renewing a key pair after inclusion on revocation list

The public keys in organisation certificates and the private keys in the microchip cannot be renewed. The creation of new key pairs requires a new organisation certificate.

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

3.4 Identification of the requester of revocation

The holder of an organisation certificate may have the certificate revoked before the expiration of the organisation certificate's validity period.

Revocation request procedure

Revocation requests are primarily made by the organisation's representative upon discovering that a certificate has been lost or it may have been misused. Requests can also be made by e.g. the card manufacturer or the registration authority.

The revocation request must be made immediately upon suspecting the misuse of a certificate, for example because of loss or theft. Organisation certificates can be revoked by calling the free revocation service at +358 800 162 622.

All revocation requests, reasons for revocation, the method of identifying the requester, and the CA's response to the request are archived.

Identification of the party requesting revocation of an organisation certificate

The caller is identified by verifying his/her personal information. If the caller is not the holder of the certificate being revoked, both the caller and the certificate holder must be identified.

The unique identifier of the certificate which is needed for the revocation request is determined from the certificate holder's identification details.

If the revocation request is made by a registration authority or a card manufacturer, identification is done according to the process described in section 4.4.3.

4 Operational requirements

4.1 Applying for a certificate

The rights and obligations of a certificate applicant are specified in contract documents and general instructions for use, which comprise an agreement concluded with the certificate applicant. The application document contains the details of the rights and obligations of both parties. When an applicant for an organisation certificate applies for an organisation certificate, he/she also accepts the general terms of use.

The application document and instructions for use clearly state that the applicant for organisation certificate, with his/her signature, approves the correctness of the information provided and the creation of the certificate and its publication in the public directory. At the same time, the applicant accepts the rules and terms pertaining to the use of the organisation certificate and sees to the storage of organisation certificates and PIN codes and the reporting of any misuse or lost certificates/microchip.

Agreements have been concluded between the certification authority and registration authority, card manufacturer and other vendors that produce parts of the certificate services, indisputably specifying the rights, liabilities and obligations of both parties.

Applications for an organisation certificate are made in person by visiting the registration authority's registration point. The applicant's identity is verified from an 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 method of identification is recorded in the application form and confirmed by signature by the registration clerk. In accordance with the agreement made with the client organisation, certificate applications can also be made using a certificate issued by PRC after 1 March 2010.

4.2 Granting of a certificate

The certification authority grants an organisation certificate upon accepting the application for certificate.

When granting an organisation certificate, the certification authority is responsible for its data content being correct at the time of delivery of the certificate.

4.3 Receiving a certificate

The organisation certificate is delivered to the certificate holder according to the certificate service procedure agreed with the organisation in question. The general terms and conditions and instructions for the use of the card are given to the certificate holder.

At the time of handing out the card, it is emphasised to the certificate applicant that there are no copies of the private signature keys created in the technical component of the card and no copies can be made later.

4.4 Termination and interruption of the validity of a certificate

4.4.1 Prerequisites for revoking a certificate

An organisation certificate must be included in a revocation list when there is reason to suspect misuse, for example because of loss or theft. Organisation certificates can be revoked by calling the free revocation service. The revocation request must be made immediately upon suspicion of potential misuse.

It is the responsibility of the organisation certificate holder to prevent the use of private keys and the related PIN codes belonging to him/her in a way contradictory to the terms of use by taking care of the card and PIN codes as set forth in the terms of use.

4.4.2 Requester of revocation

Certificate revocation requests are primarily made by the certificate holder or the organisation's contact person. If the caller is not the holder of the certificate being revoked, both the caller and the certificate holder must be identified.

Revocation requests can also be made by the certification authority, card manufacturer or registration authority. The method of identifying the person requesting the revocation is recorded.

The reasons for revocation, the date and time, and the request handler's details are recorded.

4.4.3 Revocation transaction

Certificates can be revoked by the following methods:

By calling the revocation service

By visiting the registration authority

Information of the inclusion of a certificate on a revocation list will be publicly available within an hour of the revocation request having been deemed valid and approved. The revocation list is valid for eight hours.

Revocation of an organisation certificate

The certificate holder is responsible for revoking certificates. Upon the certificate holder's notification, the organisation certificate can be placed on the revocation list to prevent its use. However, any other applications stored in the card platform can still be used according to their designated purpose.

Certificates can be revoked by calling the free revocation service on +358 800 162 622 or the textphone service for hard-of-hearing on +358 100 2288. The certificate holder's liability ends upon receipt of an identifiable notification that enables the revocation. The certificate holder's liability for the use of the certificate ceases at the same time. If necessary, the notification can be given by another person, in which case the caller's identity and connection with the ID card holder must be ascertained.

The revocation service confirms to the requester during the call when the revocation has been completed successfully.

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.

Revoked certificates cannot be reinstated.

Revocation of a certificate by the Population Register Centre

PRC revokes a certificate belonging to a deceased person upon receiving notice of the death.

The Population Register Centre will revoke a certificate issued by it if an error is found in its data content.

Population Register Centre may revoke certificates signed with its private key if there is reason to believe that Population Register Centre’s private keys have become disclosed or accessed by unauthorised parties.

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

If the private key used by the Population Register Centre in certificate creation or another technical method has become exposed or otherwise unusable, the Population Register Centre must duly notify all cardholders and the Finnish Communications Regulatory Authority of the event.

Population Register Centre may also revoke a certificate for other special reasons.

4.4.4 Timing of a revocation event

Certificates are revoked immediately in connection with a revocation request. Revoked organisation certificates cannot be reinstated.

4.4.5 Requirements for terminating the validity of a certificate

An organisation certificate cannot be temporarily suspended unless such a procedure has been specifically agreed upon between PRC and the client organisation.

4.4.6 Creator of revocation request

An organisation certificate cannot be temporarily suspended unless such a procedure has been specifically agreed upon between PRC and the client organisation.

4.4.7 Making a revocation request

An organisation certificate cannot be temporarily suspended unless such a procedure has been specifically agreed upon between PRC and the client organisation.

4.4.8 Limitations of the revocation period

An organisation certificate cannot be temporarily suspended unless such a procedure has been specifically agreed upon between PRC and the client organisation.

4.4.9 Publishing frequency of the revocation list

Information of the inclusion of a certificate on a revocation list will be publicly available within an hour of the revocation request having been deemed valid and approved. The revocation list is valid for eight hours.

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

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

In case of system updates and other exceptional situations, PRC has published revocation lists at a different frequency and extended validity periods.

4.4.10 Revocation list requirements

The obligations of a party trusting the certificate are described in section 2.1.4.

4.4.11 Online certificate status check

The certification authority provides an online certificate status check service that implements OCSP. The certification authority publishes a revocation list of revoked certificates.

4.4.12 Requirements related to online certificate status check

The certification authority provides an online certificate status check service that implements OCSP.

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

It is the certificate holder's responsibility to protect the use of their private keys by taking care of their microchip or card and PIN codes as described in the instructions for use. The certificate holder must immediately notify the revocation service if he/she suspects that his/her certificate(s) may have been used in breach of the terms and conditions.

4.5 System supervision

For supervision purposes, the certification authority stores log data about certificate production events, the certificate system's access management, hardware configuration, system software and application software, their changes, backups and recoveries. In addition, the CA supervises documents related to the activity. Any non-conformances will be reported as agreed.

4.6 Archiving of data pertaining to organisation certificates

4.6.1 Material stored

The provisions of the Archive Act (831/1994) are applied as the general law for archiving. The right to obtain information is determined according to the Act on the Openness of Government Activities (621/1999). With respect to the archiving of certificates, the provisions pertaining to archiving in electronic services legislation are also applied. Certificate register data are held for at least 5 years after expiry of the certificate. The certification authority archives the following information:

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

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

c) Events related to the creation or renewal of the CA's private key.

d) Certificate revocation requests.

e) Revocation lists submitted to the public directory and other information related to certificate revocation.

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

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

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

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

4.6.2 Protection of archives

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

4.6.3 Backup methods for archived data

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

4.6.4 Acquisition and backup methods for archived data

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

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

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

4.7 Management of the continuity of operations and handling of deviations

Population Register Centre has a continuity and preparedness plan that enables the continuity of the operations of Population Register Centre.

4.7.1 The certification authority's private key has been compromised or the certification authority's certificate has been revoked

In each certification practice statement, the certification authority states the measures that the certificate holders, parties trusting the certificate and registration authorities and the certification authority's staff must take if the certification authority's private key has become disclosed or otherwise unusable.

In such cases, the certification authority will either suspend its service as described in section 4.8 or carry out the following measures:

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

b) The certification authority creates a new key in accordance with Chapter 6.

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

d) The certification authority archives the required data as per section 38 of the Act on Strong Electronic Identification and Electronic Signatures for the statutory period and otherwise complies with the Archives Act.

4.7.2 Compromised security because of a natural disaster or other catastrophe

Population Register Centre's security policy takes into account the measures necessitated by the compromising of external security. Population Register Centre is ISO/IEC 27001 certified with

respect to information security, setting the requirements for Population Register Centre's operations also after the occurrence of a catastrophe. The Population Register Centre will comply with the procedures referred to in section 4.7 as regards the issuance and maintenance of certificates.

4.8 End of the certification authority's operations

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

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

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

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

b) The certification authority will revoke all authorisations of its contractual partners to carry out tasks pertaining to the granting process of certificates on behalf of the certification authority.

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

d) The certification authority is responsible for the archiving of the required data as per section 38 of the Act on Strong Electronic Identification and Electronic Signatures and otherwise complies with the Archives Act.

5 Physical, operational and staff security requirements

An information security certificate has been granted to Population Register Centre, affirming that PRC's information security meets the requirements of the ISO/IEC 27001 standard.

Population Register Centre uses technical vendors for carrying out the information technology tasks of the certificate service. PRC is responsible, as the certification authority, for the safety and operation of certificate production in an appropriate way in all of its sub-areas.

The Population Register Centre adheres to good information management practices. Services related to certificate provision are organised within the Certificate Services unit of the PRC.

5.1 Arrangements related to physical security

5.1.1 Location and building properties

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

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

5.1.2 Physical access to facility

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

5.1.3 Electricity supply and air conditioning

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

5.1.4 Fire safety

The data centre facilities are fitted with the necessary fire alarm mechanisms, first-aid fire-fighting equipment, and automatic fire extinguishers.

5.1.5 Data storage

Archive data and backup copies are stored separately away from the CA's hardware systems.

Data are protected against loss, modification and unauthorised use.

5.1.6 Handling of redundant data

Classified data are destroyed using reliable techniques.

5.1.7 Water damage

The data centre facilities are fitted with appropriate humidity detectors.

5.1.8 Auxiliary arrangements

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

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

5.2 Operational requirements

5.2.1 Division of responsibility

Population Register Centre uses technical vendors for the registration and information technology duties of certificate production. Population Register Centre serves as the certification authority that is responsible for certificate activities.

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

Data security

Registration

System administrator

System user

System supervisor

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

5.2.2 Number of staff required for the duties

The creation, activation, backup and recovery of the certification authority’s private key are carried out under supervision when two persons authorised to carry out maintenance on the system are present.

The revocation of the certification authority’s private key is possible only under the supervision of two authorised persons.

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

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

The registration and identification of an organisation certificate requires the presence of one person.

5.2.3 Task-specific identification

The registration authority of the organisation certificate:

The registration authority is an organisation which has a registration agreement with the Population Register Centre.

The certificate system administrator:

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

Certificate system user:

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

5.3 Personal security

Population Register Centre serves as the certification authority that is responsible for certificate activities. The technical vendors have been selected through competition and work at the responsibility and on behalf of Population Register Centre.

Population Register Centre pays particular attention to the reliability of both its own staff and the technical vendors and registration authorities and to their skills needed for the execution of the tasks.

5.3.1 Carrying out a background check on the staff

Population Register Centre has a basic security clearance done for its staff and the persons of the technical vendors who work with the certificate information system.

5.3.2 Procedure adhered to in the security clearance

Employees' work experience is mapped during the recruitment stage, and each applicant completes a form which is submitted to the Finnish Security Intelligence Service for background check purposes.

All relevant personnel of the certification authority, certificate service and directory service providers, revocation service, and the card manufacturer must:

complete a form which is submitted to the Finnish Security Intelligence Service for background check purposes;

refrain from duties which are in conflict with their obligations and responsibilities;

not be persons known to have been released from a previous duty on the grounds of negligence of duty or misconduct;

be appropriately qualified for the duties they are taking on.

5.3.3 Requirements on training

Population Register Centre's staff must be trained so that duties can be carried out in the best possible way. Population Register Centre has a training plan the implementation of which is the responsibility of Population Register Centre’s administration unit.

5.3.4 0.0.1.Maintenance of expertise and skills

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

5.3.5 Requirements for task rotation

When task rotation is planned for the certification authority’s tasks, they must be organised in such a way that the person can see to his/her new duties in the best possible way. The implementation of task rotation must also take into account the retention of good information administration practice and the maintenance of sufficient task-specific skill levels.

Task rotation also adheres to Population Register Centre's information security policy and information security plan as well as Population Register Centre's other general instructions.

5.3.6 Measures resulting from deviations

Population Register Centre's staff work subject to official liability and in accordance with the internal instructions of Population Register Centre. The position of a public official is set forth in the State Officials Act (750/1994).

5.3.7 Staff representing the organisation

When recruiting staff, it must be seen to that the staff’s skills correspond to the requirements of the task and that there is nothing detected in the person's background check that would put the person's interests at odds with the production of certificate services.

5.3.8 Documents given to the staff

The staff always has access to Population Register Centre's quality and security documents.

6 Technical security arrangements

6.1 Generation and storage of key pairs

6.1.1 Generating key pairs

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

Certification authority:

The certification authority generates its private signature keys and corresponding public keys. The keys are stored in hardware security modules administered by the certification authority. The modules meet the FIPS 140-1 Level 3 requirements.

Certificate holder:

Keys can be created by batch processing before certification or directly in conjunction with it. In both cases, the private key is kept read- and write-protected on the ID card.

The certification authority creates the certificate holder's keys within the ID card. No copy of private signature keys is made.

6.1.2 Delivery of a private key to certificate holder

The ID card, which contains the certificate holder's private keys and requires the original PIN codes in order to be activated, is delivered to the client by a method which ensures that the card is not physically in the same place as the PINs before it reaches the client. This is done by using separate routes of transmission and by delivering the card and the PINs at different times.

The card is handed over to the card holder in person at the service point of the registration authority representing the certification authority. The organisation certificate holder must prove his or her identity in accordance with the procedure used in the application stage. The method of identification is recorded in the receipt note, which is signed by the customer and the registration authority's representative who hands over the ID card.

6.1.3 Delivery of the certificate holder’s public key to the certification authority

The integrity of public keys is protected until certification is performed. Once keys are generated, the card manufacturer submits certificate requests to the certificate system. The certificate request includes the public key and other certificate data. The connection between the certificate request system and the certificate generation system is encrypted, and persons who boot the system are identified with management cards issued by the certification authority.

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

The certification authority's public key is held in the CA certificate, which is located on an ID card. The CA certificates are freely distributable and available in a public directory and the CA's online service.

6.1.5 Key lengths

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

The certificate holder's private and public keys are 2048-bit RSA keys at minimum.

6.1.6 Intended use of keys

The data content of the certificate has a field that determines the intended use of the related key (e.g., authentication and encryption or digital signing). The use of the key is restricted to its intended use. For example, a key intended for digital signing must be used only for this purpose and not for authentication and encryption.

CA certificate:

Purpose: Signing of certificates and revocation lists. The technical description is in the FINEID S2 specifications.

Certificate holder's authentication and encryption certificate:

Purpose: Electronic identification or data encryption.

Certificate holder's signature certificate:

Purpose: Digital signature.

6.2 Protection of private key

6.2.1 Standards for the hardware security module

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

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

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

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

6.2.3 Disclosure of private key to a trusted party

Cardholders' private keys are generated in a secure way as required by the Regulation. Key pairs generated by the card holder are not accepted. A private key cannot be transferred or copied from an ID card. The certification authority or the card manufacturer are not able to access the private keys of users. Signature keys stored on ID cards do not have the so-called key recovery function. Key recovery can be performed on the authentication and encryption certificate in accordance with the agreement made between PRC and the certificate client organisation. When the keys are generated, they have not been allocated to any person.

6.2.4 Backup of a private key

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

6.2.5 Archiving of private keys

The certification authority’s private keys are stored in hardware security modules administered by the certification authority.

6.2.6 Administration of private keys in hardware security modules

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

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

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

6.3 Other key management issues

6.3.1 Public key archiving

The certification authority archives all public keys it has certified.

6.3.2 Usage period of public and private keys

The usage period of an organisation certificate is determined by the agreement in question; a typical period is 2–5 years. The certificate can be revoked during its validity. Certified signatures created before the revocation or expiry of the certificate can still be verified after the revocation or expiry from data stored in the certificate.

6.4 Activation data

6.4.1 Creation and commissioning of activation data

The card manufacturer creates activation data, i.e., PIN codes, that enables the use of the keys. Individual PIN codes and PUK codes are computed and transferred on to the card and, in encrypted form, on to a response file for transfer into the card manufacturer's production system. When the cards have been delivered, the corresponding encrypted PIN and PUK codes are transferred to a department that is separate from card manufacturing, where the PIN and PUK letters are then printed. The letters are sent to the address given by the applicant in the card application once the agreed period of time has elapsed since the cards were sent.

6.4.2 Protection of activation data

PIN codes are protected so that they cannot be read or copied from the card. It is the certificate holder's responsibility to protect the use of his/her keys by taking care of his/her card and PIN codes as described in the terms and conditions of use.

6.4.3 Other activation data issues

It is explained to the holder of an organisation certificate that he/she has the possibility to change the original PIN codes to new ones. The program for changing the PIN code is available free of charge for the cardholders at www.fineid.fi.

An ID card will be locked and blocked after three incorrect PIN entry attempts. A locked PIN code can be released by contacting the registration authority. After unlocking, the unlocking codes are deleted from the memory of the system used to unlock the code.

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

6.5.1 Hardware security

Only equipment suitable for their intended use is used in the certificate system.

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

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

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

The certificate system hardware is under 24-hour security monitoring.

6.6 Certificate system life cycle management

Population Register Centre maintains a classification of importance on certificate service objects and systems, their backups, priorities and minimum maintenance levels.

6.6.1 Supervision related to developing the system

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

6.6.2 Security management

Population Register Centre's information security is managed according to Population Register Centre's information security policy and the standard ISO/IEC 27001.

6.7 Telecommunication network security

The security of telecommunication is implemented in such a way that the certificate system's telecommunication network is a consistent whole isolated from other telecommunication networks and has doubled critical components. Transmitted messages, their senders or recipients cannot be viewed by unauthorised parties without special measures. The network is only used for tasks related to the certificate system. Redundant network services have been disabled. The network is divided into logical sub-components with restricted connectivity between components. Sufficient authentication, access control and non-repudiation procedures are in place.

6.8 Monitoring of the use of the hardware security module

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

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

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

7 Certificate and revocation list profiles

7.1 Technical certificate data

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

7.2 Revocation list profile

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

8 Specification document management

8.1 Changing of specifications

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

8.2 Publishing and communication

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

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

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

8.3 Certificate policy change and approval procedure

Population Register Centre approves the certificate policy and certification practice statement pertaining to organisation certificates. The documents may be amended according to Population Register Centre's internal change policy.

Population Register Centre will communicate the changes to FICORA and on its own website well in advance of their entry into force.

Population Register Centre maintains version management of the documents and archives all certificate policy and certification practice statement documents. Typographic corrections and changes of contact details are possible with immediate effect.

After 28 September 2017, all items of the certificate policy and certification practice statement can be amended by communicating the main upcoming changes 30 days before their entry into force.

Further, after 28 September 2017, items that Population Register Centre does not deem to have significant effect on certificate holders and trusting parties may be amended with communication 14 days in advance.