Väestörekisterikeskus
Befolkningsregistercentralen

Certificate policy

for Root Certificate

OID: 1.2.246.517.1.10.1

v.1.4

SERTIFIOITU inspecta ORGANISAATIO
ISO 9001

SERTIFIOITU inspecta ORGANISAATIO
ISO/IEC 27001

Contents

1. Introduction 3
1.1. General points 3
1.2. Identifiers 4
1.3. The root certification authority and the range of application of CA certificates 4
1.3.1. Root certification authority 5
1.3.2. Registration authority 5
1.3.3. Directory service 5
1.3.4. CA certificate holder organisation 5
1.3.5. Trusting a CA certificate 5
1.3.6. Using a CA certificate 5
1.4. Contact details 5
1.4.1. Organisation administering the certificate policy 6
1.4.2. Contact person 6
2. General terms and conditions 6
2.1. Obligations 6
2.1.1. The obligations of the root certification authority 6
2.1.2. The obligations concerning the CA certificate holder organisation 7
2.1.3. Responsibilities of the party relying on a CA certificate 7
2.1.4. Obligations pertaining to the publishing of a CA certificate 7
2.2. Liabilities 7
2.2.1. Root certification authority's responsibilities 8
2.2.2. Registration authority's responsibilities 8
2.2.3. CA certificate holder organisation's responsibilities 8
2.2.4. Responsibilities of a party relying on a CA certificate 8
2.2.5. Limitations of liability 8
2.3. Financial liability 9
2.3.1. Root certification authority 9
2.3.2. Other parties 9
2.3.3. The root certification authority's financial administration 9
2.4. Interpretation and implementation 9
2.4.1. Applicable legislation 9
2.4.2. Settling of disputes 9
2.5. Fees 10

2.5.1. Issuing and renewing a CA certificate 10
2.5.2. Fees related to the use of a CA certificate 10
2.5.3. Fees related to the revocation of a CA certificate 10
2.6. Publishing and availability of data 10
2.6.1. Publication of CA certificate data 10
2.6.2. Publication frequency 10
2.6.3. Availability of data 10
2.6.4. Repositories 10
2.7. Information security audit 10
2.7.1. Audit frequency 11
2.8. Publication of data 11
2.8.1. Information published by the root certification authority 11
2.8.2. Other principles concerning disclosure of information 11
2.9. Intellectual property rights 11
3. Identification of CA certificate applicant 11
3.1. Registration 11
3.1.1. Naming policies 12
3.1.2. Delivery of private keys to the CA certificate holder 12
3.2. Renewal of key pair 12
3.3. Making a revocation request 12
4. Operational requirements 12
4.1. Applying for a CA certificate 13
4.2. Issuing a CA certificate 13
4.3. Receiving a CA certificate 13
4.4. The validity and revocation of a CA certificate 13
4.4.1. Prerequisites for revoking a CA certificate 13
4.4.2. Publishing frequency of the revocation list 14
4.4.3. Special requirements pertaining to the exposure of the CA certificate holder's private key 14
4.5. System supervision 14
4.6. Archiving of data pertaining to CA certificates 14
4.6.1. Material stored 14
4.7. Continuity management and handling of deviations 14
4.8. End of the root certification authority's operation 14
5. Physical, operational and staff security requirements 15

6. Technical security arrangements 15
6.1. Generation and storage of key pairs 15
6.1.1. Generating key pairs 15
6.1.2. Key lengths 15
6.1.3. Intended use of keys 15
6.2. Protection of private key 15
6.3. Other key management issues 16
6.4. Security requirements pertaining to the use of and access to computers ... 16
6.5. Certificate system life cycle management 16
6.6. Telecommunication network security 16
6.7. Monitoring of the use of the hardware security module 17
7. CA certificate and revocation list profiles 17
7.1. Technical specifications of CA certificates 17
7.2. Revocation list profile 17
8. Specification document management 17
8.1. Modifications to specifications 17
8.2. Publication and communication 17
8.3. Certificate Policy modification and approval procedure 17
8.4. Version management 18

Definitions and abbreviations

Definitions

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

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

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

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

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

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

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

Citizen certificate: A certificate for secure use of e-services issued by the Population Register Centre to a natural person governed by the Act on the Population Information System and the Certificate Services of the Population Register Centre (661/2009).

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

Qualified certificate: A certificate whose data content is compliant with the content specified for a qualified certificate and which has been issued by a certification authority issuing qualified certificates that meets the legal requirements. The data content of a qualified certificate is laid down in section 7 of the Act on Strong Electronic Identification and Electronic Signatures (617/2009).

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

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

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

Service certificate: A file-based certificate intended for such purposes as receiving and sending encrypted e-mails using a shared mailbox as well as certifying a server (server certificate).

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

RSA algorithm: An asymmetric public key algorithm.

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

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

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

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

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

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

Certificate register: A register compliant with section 14 of the Act on Strong Electronic Identification and Electronic Signatures that a certification authority providing qualified certificates to the public must maintain. The data must be held for 10 years after the expiry of the certificate.

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

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

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

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

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

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

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

Acronyms

ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practise Statement
CRL	Certificate Revocation List
FINEID	Finnish Electronic Identification
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module

eID	Electronic identification of a person
HTTP	Hypertext Transfer Protocol
ISO 27001	ISO IEC 27001
LDAP	Lightweight Directory Access Control
OCSP	Online Certificate Status Protocol, an online service for checking the status of a certificate
OID	**Object Identifier**
PDS	PKI Disclosure Statement, certificate description
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman
SIM	Subscriber Identity Module
PRC	Population Register Centre

1. Introduction

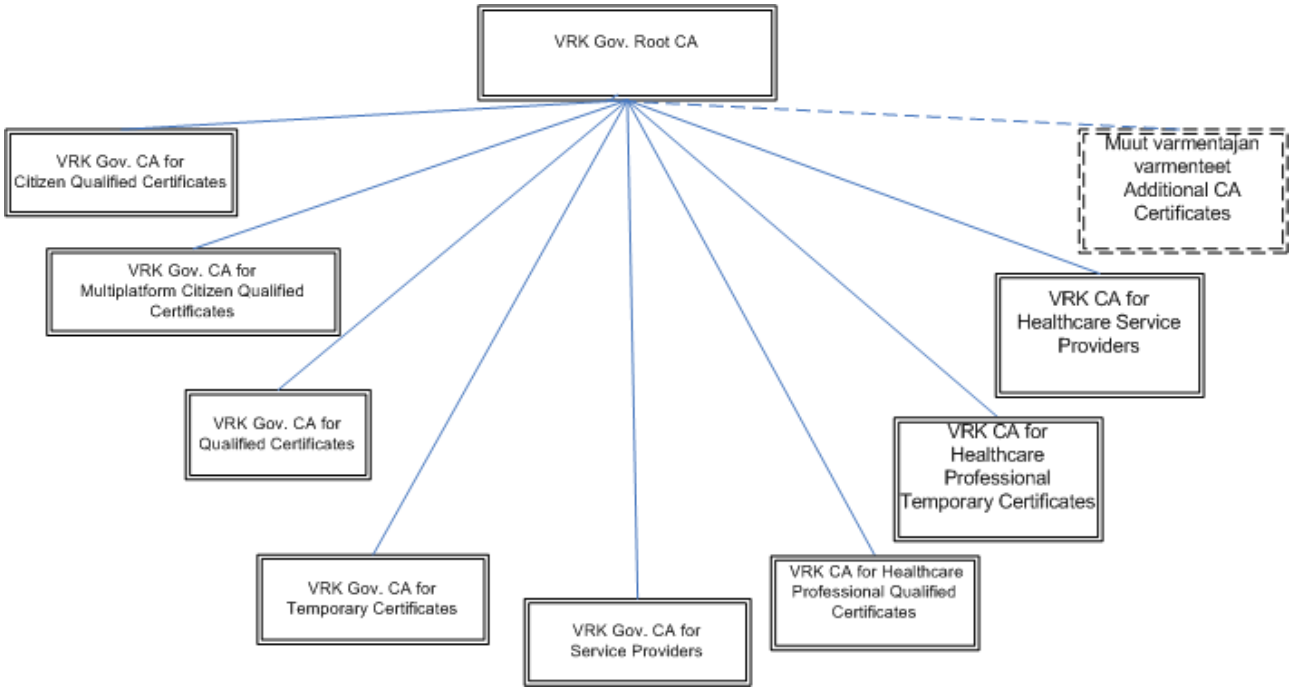
A certificate policy is a document drawn up by a certification authority (CA) which describes the practices and principles used in certification. The certification practice statement is a more detailed description of the certification authority's activities than a certificate policy.

This certificate policy is applied as the root certificate authority (PRC Gov. Root CA) issues CA certificates.

1.1. General points

The Population Register Centre introduced a new certificate system on 31 March 2003. The Population Register Centre's trust model is hierarchic: the PCR has a single root certification authority that issues certificates to other certification authorities. A certification authority may be either the Population Register Centre or some other public or private organisation.

This document describes the practices that the root certification authority follows when issuing CA certificates to either the Population Register Centre or some other organisation. The root certification authority does not grant end user certificates. End user certificates are issued by certification authorities certified by the root certification authority, each of which have their own certificate policies and certification practices.



The CA certificate includes the CA's public key, name, the intended use of the certificate as well as other information necessary for the use of the certificate. The certificate data are signed electronically by the root certification authority's private key. CA certificates under this certificate policy are based on a public key infrastructure.

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

The Population Register Centre's Certificate Policy and Certification Practice documents have unique identifiers (OIDs).

The Population Register Centre draws up a certificate policy for the root certification authority and separate certificate practice statements for each type of CA certificate issued by the root certification authority.

The Certificate Policy contains a general description of the practices, terms and conditions, responsibility allocation and other matters related to certification for each type of certificate in the Population Register Centre's certification activities. The Certification Practice Statement contains a detailed description of the applicable practices.

1.2. Identifiers

The title of this certificate policy is Certificate Policy for CA Certificates, and its unique identifier is OID 1.2.246.517.1.10.1.

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

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

The root certification authority provides certificate services according to the terms and conditions specified in this certificate policy and guarantees their functioning in accordance with Chapter 2.2.1 on the responsibilities of the root certification authority. The root certification authority is responsible for the functioning of the CA certificate system as a whole, including any registration authorities and technical suppliers it may use. This certificate policy has been registered by the

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

1.3.1. Root certification authority

The task of the root certification authority is to:

issue CA certificates

ensure the accuracy of the data content of the certificates issued by it

provide certificate and directory services in accordance with its certificate policy and certification practice statement, and certification revocation services

revoke certificates and publish certificate revocation lists.

1.3.2. Registration authority

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

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

1.3.3. Directory service

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

1.3.4. CA certificate holder organisation

This certificate policy describes the root certification authority's procedure for issuing CA certificates for the use of the Population Register Centre or some other organisation.

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

1.3.5. Trusting a CA certificate

The party relying on a CA certificate is a person or an organisation that trusts the CA certificate data. The trusting party must verify that the CA certificate is valid and not on a revocation list.

1.3.6. Using a CA certificate

In accordance with this certificate policy, the root certification authority issues CA certificates as described in the certification practice statement for the relevant CA certificate. The purposes of using CA certificates include signing citizen certificates and signing the certificate revocation list.

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

1.4. Contact details

1.4.1. Organisation administering the certificate policy

This certification practice statement was registered by the Population Register Centre. The centre is responsible for the administration and updating of this certificate policy.

1.4.2. Contact person

Questions regarding this Certificate Policy should be addressed to:

Population Register Centre	vaestorekisterikeskus@vrk.fi
P.O. Box 123 (Lintulahdenkuja 4)	Tel. +358 295 535 001
FI-00531 Helsinki	Fax. +358 9 876 4369
Business ID: 0245437-2	

Questions regarding the certificate policy are handled by the Certificate Services unit of PRC.

2. General terms and conditions

This certificate policy is effective as of 01/12/2010. The modification and publication procedure of the policy is described in Chapter 8 of this document.

2.1. Obligations

2.1.1. The obligations of the root certification authority

The root certification authority shall act in compliance with current legislation.

The root certification authority performs its duties carefully, reliably and appropriately.

The root certification authority must have the necessary technical capabilities, financial resources and ability to cover its liability for damages.

The root certification authority is responsible for all areas of the certification activity, including the reliability and functioning of the services and products produced by any technical suppliers or persons who assist the root certification authority.

The root certification authority draws up and maintains a Certificate Policy which describes at a general level the procedures for issuing, maintaining and managing CA certificates, the terms and conditions, the allocation of responsibilities, and other matters related to the use of CA certificates.

The root certification authority draws up and maintains certification practice statements which describe how the root certification authority applies its certificate policy.

The root certification authority complies with the certificate policy and certification practice statement requirements.

The root certification authority makes the certificate policy and the certification practice statement publicly available.

The root certification authority shall employ sufficient staff with the expertise, experience and competence required for producing certificate services.

The root certification authority shall use reliable systems and products protected against unauthorised use.

The root certification authority keeps publicly available information regarding its root certificates and certificate activities, based on which the operation and reliability of the root certification authority can be assessed.

The root certification authority complies with the certificate policy and the certification practice statement in registration.

The root registration authority identifies the CA certificate applicant reliably as described in the certification practice statement, ensuring that the applicant's information is carefully verified.

The root registration authority shall see to the careful handling and confidentiality of the data.

2.1.2. The obligations concerning the CA certificate holder organisation

The intended use of the CA certificate is described in the certification practice statement for the relevant CA certificate. The certificate may only be used for the intended purpose.

An organisation that holds a CA certificate is responsible for ensuring that the data provided in the certificate application is correct.

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

The CA certificate holder organisation must notify the root certification authority immediately if it knows or suspects that the CA certificate holder's private key has been compromised. The root certification authority will then revoke the CA certificate in question and publish it on the revocation list.

2.1.3. Responsibilities of the party relying on a CA certificate

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

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

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

If the most recent revocation list cannot be retrieved from the directory because of hardware or directory service malfunction, no certificate should be accepted if the validity period of the last retrieved revocation list has expired. All CA certificate and end user certificate approvals after the validity period are at the risk of the party trusting the CA certificate.

2.1.4. Obligations pertaining to the publishing of a CA certificate

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

2.2. Liabilities

2.2.1. Root certification authority's responsibilities

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

The root certification authority ensures that the CA certificate will be available from the time it is handed over for its entire period of validity, unless the CA certificate has been reported to the revocation list.

The root certification authority ensures that the CA certificate has been released according to agreement to the organisation identified as required by the CA certificate.

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

2.2.2. Registration authority's responsibilities

The root certification authority serves as the CA certificate's registration authority. The root certification authority is liable for the damages pertaining to registration in accordance with this section.

2.2.3. CA certificate holder organisation's responsibilities

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

The CA certificate holder organisation's responsibility for the certificate use ends when it has provided the root certification authority with the information on revoking the certificate in accordance with the agreement concerning the issue of the CA certificate. To end the responsibility of the CA certificate holder organisation, the revocation request must be made immediately after giving the reason for making the request.

2.2.4. Responsibilities of a party relying on a CA certificate

A party relying on a CA certificate may not trust the correctness of a CA certificate in good faith if the validity of the certificate has not been checked against the revocation list. Accepting the CA certificate in the above cases releases the Population Register Centre from liability and responsibility. A party trusting a CA certificate must verify that the certificate issued corresponds to its intended use

2.2.5. Limitations of liability

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

The root certification authority is not liable for indirect or consequential damage caused to the CA certificate holder organisation. Neither is the root certification authority liable for indirect or consequential damages incurred by other partners of the relying party or the certificate holder organisation.

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

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

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

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

The CA certificate holder organisation's responsibility for certificate use ends when a representative of the organisation has provided the root certification authority with the information required to revoke the certificate. You should make the revocation request immediately after you have noticed the reason for making the request.

2.3. Financial liability

2.3.1. Root certification authority

The root certification authority's liability for damages in connection with certificate service provision is determined on the basis of the Tort Liability Act (412/1974).

2.3.2. Other parties

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

2.3.3. The root certification authority's financial administration

The certificate services produced by the Population Register Centre, which acts as the root certification authority, are covered by a financial administration system and supervision as has separately been set forth. The Population Register Centre is an agency subject to net budgeting operating under the Ministry of the Interior. Some two thirds of its expenditure are covered by the fees collected for its services. The financial management of the Population Register Centre is based on the acts and decrees that govern central government finances and regulations issued by the Ministry of Finance and the State Treasury. The National Audit Office is responsible for the PRC's financial oversight. In addition, its performance is reviewed from the points of view of effectiveness, economy and productivity.

2.4. Interpretation and implementation

2.4.1. Applicable legislation

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

Provisions on the Population Register Centre's position are laid down in the register administration act (rekisterihallintolaki 166/1996) and decree (248/1996).

2.4.2. Settling of disputes

When granting certificates, the root certification authority is responsible that the CA certificates fulfil the requirements set in this certificate policy.

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

2.5. Fees

This section specifies the fees related to the use of a CA certificate issued by the Population Register Centre.

2.5.1. Issuing and renewing a CA certificate

CA certificates are applied from the Population Register Centre. A certificate is always issued against a new application, following the identification procedure specified in the Certification Practice Statement. The price of the CA certificate is based on the valid annual fee indicated in the Population Register Centre's service price list.

2.5.2. Fees related to the use of a CA certificate

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

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

2.5.3. Fees related to the revocation of a CA certificate

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

2.6. Publishing and availability of data

2.6.1. Publication of CA certificate data

The root certification authority publishes all CA certificates and revocation lists in a public directory with open access. The Population Register Centre publishes the Certificate Policy, the Certification Practice Statements, the PDSs and other public documents pertaining to the production of certificate services on its website.

2.6.2. Publication frequency

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

2.6.3. Availability of data

Access to the directory and the revocation list data is open. The FINEID specifications, Certificate Policies and Certification Practice Statements published by the Population Register Centre can be accessed on the Centre's website.

2.6.4. Repositories

The data published by the Population Register Centre, which acts as the root certification authority, is available on the Centre's website. Any non-public certificate system data is saved in the Population Register Centre's repository. A root certification authority's data is archived according to the authority's valid archiving rules.

2.7. Information security audit

2.7.1. Audit frequency

As the root certification authority, the Population Register Centre carries out information security audits that cover the facilities, hardware and activities of the holder organisation as appropriate. An audit is carried out at least once a year and at the start of each new contract period. In its audit procedure, the Population Register Centre adheres to the practices set out in the ISO 27001 information security management standard.

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

2.8. Publication of data

2.8.1. Information published by the root certification authority

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

The data in 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.

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

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

The data in the certification system is only disclosed for the purposes referred to in this section.

2.8.2. Other principles concerning disclosure of information

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

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

2.9. Intellectual property rights

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

3. Identification of CA certificate applicant

3.1. Registration

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

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

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

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

3.1.1. Naming policies

The root certification authority is:

CN (Common name) = VRK Gov. Root CA

OU (Organizational unit) = Certificate Services

OU (Organizational unit) = Certification Authority Services

O (Organization) = Vaestorekisterikeskus CA

S (State) = Finland

C (Country) = FI

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

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

3.1.2. Delivery of private keys to the CA certificate holder

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

3.2. Renewal of key pair

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

3.3. Making a revocation request

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

A representative of the CA certificate holder organisation must notify the root certification authority immediately in the manner specified in the delivery contract if they know or suspect that the CA certificate's private key has been compromised. The root certification authority will then revoke the relevant CA certificate. Revocation requests are primarily made by CA certificate holders if the certificate may have been misused. Revocation requests can also be made by the registration authority or the root certification authority.

4. Operational requirements

4.1. Applying for a CA certificate

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

4.2. Issuing a CA certificate

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

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

4.3. Receiving a CA certificate

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

4.4. The validity and revocation of a CA certificate

4.4.1. Prerequisites for revoking a CA certificate

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

Revoked CA certificates cannot be reinstated.

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

The root certification authority may revoke CA certificates signed with its private key if there is reason to believe that the root certification authority's private keys have become disclosed or accessed by unauthorised parties.

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

If the private key used by the Population Register Centre in issuing a CA certificate or another technical method has become exposed or otherwise unusable, the Population Register Centre must duly notify all CA certificate holder organisations and end users.

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

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

4.4.2. Publishing frequency of the revocation list

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

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

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

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

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

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

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

4.5. System supervision

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

4.6. Archiving of data pertaining to CA certificates

4.6.1. Material stored

The provisions of the archive act (arkistolaki, 831/1994) are applied as the general act on archiving. The right to obtain information is determined according to the Act on the Openness of Government Activities (621/1999). With respect to the archiving of the root certification authority's certificates, the provisions pertaining to archiving in electronic services legislation are also applied.

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

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

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

4.7. Continuity management and handling of deviations.

The root certification authority has a continuity and preparedness plan that enables the continuity of the root certification operations. For a description of the root certification authority's action when dealing with deviations, see the Certification Practice Statement.

4.8. End of the root certification authority's operation

A situation where all services related to issuing, maintaining and administrating root certification authority and CA certificates are permanently terminated is deemed the termination of the root

certification authority. The termination of the root certification authority does not refer to a situation where the root certificate service is transferred from one organisation to another. For a description of the root certification authority's action when dealing with deviations, see the Certification Practice Statement.

5. Physical, operational and staff security requirements

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

The Population Register Centre uses technical vendors for carrying out the information technology tasks of the root certification authority. As the certification authority, the root certification authority is responsible for the security and operation of certificate production in an appropriate way in all of its areas. For a detailed description of the root certification authority's action when dealing with deviations, see the Certification Practice Statement.

When an organisation other than the root certification authority issues end user certificates based on a CA certificate, the organisation also complies with its own information security policies.

6. Technical security arrangements

6.1. Generation and storage of key pairs

6.1.1. Generating key pairs

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

The root certification authority generates its private signature keys and corresponding public keys. The keys are stored in key management devices governed by the root certification authority.

6.1.2. Key lengths

The root certification authority's private key, which is used to sign the root certification authority's certificates, and the corresponding public key are 2048-bit RSA keys.

For the lengths of the CA certificate holder's public and private keys, see the certification practice statement.

6.1.3. Intended use of keys

The key usage field in the certificates specifies the intended use of the public and private keys associated with a CA certificate.

6.2. Protection of private key

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

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

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

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

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

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

6.3. Other key management issues

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

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

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

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

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

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

6.5. Certificate system life cycle management

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

In its role as a root certification authority, the Population Register Centre's information security is managed according to the Population Register Centre's information security policy and standard ISO 27001.

6.6. Telecommunication network security

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

6.7. Monitoring of the use of the hardware security module

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

The module collects log data on events.

7. CA certificate and revocation list profiles

7.1. Technical specifications of CA certificates

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

7.2. Revocation list profile

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

8. Specification document management

8.1. Modifications to specifications

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

8.2. Publication and communication

The root certification authority publishes a certificate policy and a certification practice statement, which are available on the websites www.vaestorekisterikeskus.fi and www.fineid.fi.

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

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

8.3. Certificate Policy modification and approval procedure

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

The Population Register Centre communicates on the modifications well in advance of their entry into force on its website.

The 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 may be made with immediate effect.

1. After 01/12/2010, all sections of the certificate policy and certification practice statement can be amended by communicating the main upcoming changes 30 days before their entry into force.

2. Further, after 01/12/2010, 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.

8.4. Version management

Root certification authority's certificate policy for CA certificates, v. 1.4

Version	Date	Description/modifications
v 1.0.	31/03/2003	Approved version v 1.0., published on 3 September 2004 www.fineid.fi
v 1.1.	01/01/2009	Changes brought about by structural rearrangements in central government (change of ministry); clarifying changes in the factual content
v 1.2.	01/03/2010	Act on the Population Information System and the Certificate Services of the Population Register Centre (661/2009), Act entered into force on 1 March 2010. The Act on the Population Information System and Certificate Services Provided by the Population Register Centre (507/1993) has been repealed. Act on Strong Electronic Identification and Electronic Signatures (617/2009), the act entered into force on 1 September 2009. The Act on Electronic Signatures (14/2003) has been repealed. Ministry of Finance decree on the payment of Population Register Centre fees (873/2008), decree entered into force on 1 January 2009.
v1.3	01/12/2010	Changes pertaining to authentication in healthcare (the Population Register Centre acts as the healthcare certification authority) in the act on the electronic handling of social welfare and health care customer data (159/2007), the act on electronic prescriptions (61/2007) and the act on the population information system and the Population Register Centre's certificate services (661/2009) will enter into force on 1 December 2010.
v 1.4	01/03/2013	Change of contact details