OP GROUP
CERTIFICATE POLICY

BUSINESS SERVICES ROOT CERTIFICATION AUTHORITY

OP-Pohjola Root CA

Version 3.0
Effective 6.3.2017

OID: 1.3.6.1.4.1.11374.1.1.1.1.3

CONTENTS

INTRODUCTION

Certificate Policy (CP) describes the practices and principles according to which the Certification Authority (CA) issues Certificates. Certification Practice Statement (CPS), in turn, describes the CA's activities in more detail than the CP.

The CP defines the responsible organizations related to the activities, along with their roles and responsibilities. In addition, the CP defines physical, functional, personnel-related and technical security requirements that the CA complies with in its activities.

Identification information:

OP-group, Certificate Policy, Business Services' Root CA

OID: 1.3.6.1.4.1.11374.1.1.1.1.3

1 SCOPE

This CP applies to OP-group's Certification Authority (CA), which is a dedicated Root CA. In other words, the CA is not subordinate to another Root CA or a Subordinate CA. This CA issues Certificates only to other Certification Authorities.

This policy defines basic requirements for the business and technical solutions of the Public Key Infrastructure (PKI) under the Business Services' Root CA. In addition, the policy describes the basic requisites for secure administration and use of PKI-based certificates. The policy is strongly based on standard *Policy requirements for certification authorities issuing public key certificates (*ETSI TS 102 042 v2.1.1, 2009) and the normalized CP (NCP) defined by it. This CP also adheres to, to some extent, the documents listed in "References" chapter 2.

This CA issues Subordinate CA Certificates to the following parties:

- Units and functions producing and managing OP-Group's business and ICT services.

2 REFERENCES

ETSI042	**ETSI TS 102 042** v2.1.1 (2009) Policy requirements for certification authorities issuing public key certificates.
ETSI176-1	**ETSI TS 102 176-1** v2.0.0 (2007) Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
FIPS PUB 140-2	**FIPS PUB 140-2** Security requirements for cryptographic modules
ISO 21188	**ISO 21188** (2006) Public key infrastructure for financial services – Practices and policy framework

3 DEFINITIONS, ABBREVIATIONS AND NOTATION

3.1 Definitions

Subordinate CA Certificate: A Certificate issued to a Subordinate CA.

Subordinate CA: A CA that is not a Root CA. Subordinate CA's Certificate is signed by a Root CA. (see CA and Root CA).

End-entity: In this context: Party that has made an agreement for the use of certificate services and has signed Certificate subscriber's agreement.

End-entity Certificate: A certificate issued to an End-entity by a CA. End-entity Certificate can be used for various purposes, but it nevertheless never is a CA Certificate. The Private Key of the End-entity Certificate's Key Pair is in the possession of the End-entity.

Audit trail: Requirement for log entries to be done in a manner that allows for actions done in a system to be accurately traced.

Key usage: A Certificate's technical parameter used for defining the approved usage purposes for a Certificate on a general level.

Key Pair: In Public Key Infrastructure, two keys associated with each other are used, one of which one is public and the other private. Together they form a Key Pair. The usage purpose of the keys is defined in the Certificate, which in turn is governed by the CP.

Hardware Security Module (HSM): A special device used for protecting private keys.

Public Key: The public part of the Key Pair used for asymmetric encryption in Public Key Infrastructure. Data encrypted using the public key (for example, in RSA-algorithm) can be decrypted only with the private key of the Key Pair. When the party in possession of the Public Key is known, a digital signature created with the associated Private Key can be verified. The person in possession of the Public Key can be identified reliably using the Certificate.

Public Key Infrastructure (PKI): A solution formed by technical and procedural solutions, with which Public Key Certificates are generated, managed, distributed, used, stored and revoked. The infrastructure also assigns controls and standards that Certification Authorities must conform to in their activities in order to ascertain the compatibility, identifiability and availability of the digital Certificates. PKI is based on the Public Key encryption algorithm.

Public Key Cryptography: In Public Key cryptography there are two associated keys: a Public Key and a Private Key, that together form a Key Pair. Data encypted using the Public Key can usually only be decrypted using the Keypair's Private Key. RSA algorithm also works in the opposite way: Data encrypted using the Private Key can only be decrypted using the Public Key. Digital signatures are based on this special property of the RSA and some other algorithms.

Root Certificate: A Root Certificate is a Certificate issued by a Root CA to itself and the highest level of a Certificate hierarchy (a so called trust anchor).

Root Certification Authority; Root CA: the most reliable and the first party in a hierarchical PKI Certificate chain. The Root CA defines the Certificate Policies and the technical and operational norms.

Dual Control: Principle according to which performing of certain operations must always require at least two persons. This is to stop malpractice by individual persons from taking place in security-critical functions.

Key escrow: A security mechanism, in which the encryption key is trusted to third party storage so that it can in certain circumstances be used by the third party. Key Escrow is usually associated with keys used in encryption and not with signing or authentication keys. If the Key Escrow method is used in PKI, it has to be mentioned in the associated Certification Authority's CP.

Relying Party: The party receiving the Certificate, that trusts in the information contained in the Certificate or in the information of a digital signature based on the Certificate and uses them in their activities. Relying parties include, for example, subordinate Certification Authorities, Subordinate CA-signed Certificates' subjects (end-entities), business services or other third parties using OP-group's Certificates.

Relying Party Agreement (RPA): An agreement between a CA and a Relying Party, in which the Certificate use of both parties is defined, for example, obligations and responsibilities associated with verification of digital signatures.

Principle of Least Privilege: Access rights management principle, according to which only such rights are given to an employee that are necessary for the execution of their tasks. Access rights are removed when they are no longer necessary.

Registration Authority (RA): An RA is generally responsible for functions, including, among others:

1) Identifying (confirms identity) of the Certificate Subscriber (for example, a company) and a possible representative (for example, a company representative)

2) Approves/rejects certificate signing requests.

3) When needed, starts Certificate Revocation or Suspension process.

4) Can handle a Certificate Subject's Suspension or Revocation request. Approves or rejects Certificate renewal requests and requests for a new key for an existing Certificate.

Registrar does not, however, sign or issue Certificates. Registrar performs only the tasks delegated to it by the CA.

Ceremony: An operation of predefined form approved by the CA, that, in order to be conducted, needs more than two persons present and to which a chair person is selected.

Usually ceremonies are used for key management operations, such as the generation of a CA's key.

CRL Distribution Point (CDP): CRL publishing location.

Certificate Revocation List (CRL): A list digitally signed by a CA that contains the serial numbers of revoked Certificates and the code representing the reason for their revocation.

Revocation Service: CA's service responsible for revoking and placing Certificates on hold (temporary invalidation; suspension)

Validation Authority (VA): Validation authority is a service that can be used by Relying Parties for confirming a Certificate's validity in connection with making trust decisions. In practice, Validation Authority refers to a list of revoked Certificates.

Validation Authority can offer the CRL file using different protocols or a status request service over OCSP protocol.

Digital Signature: A result of a mathematical calculation, with which a message sender's or a document signer's identity and the integrity of the content is authenticated. In other words, a digital signature ties a message to its sender. In this context, the term refers to the technical method of adding a digital signature in all use cases, and not to digital signature itself as it is defined in the act on Strong Electronic Identification and Electronic Signatures.

Subscriber: see Certificate Subscriber.

Segregation/Separation of Duties: Practice, in which tasks related to a certain function have been divided between several people so that no one can independently abuse the process.

Certificate: A data structure that associates a Public Key to its subject's information and that has been signed with the Certificate issuer's (CA) private key.

Certificate Chain: With the Certificate chain one can, by trusting the Root Certificate, verify the chain's Certificates and make a trust decision regarding an End Entity's Certificate

Certificate Chain begins from a Root Certificate and ends at an End-entity's Certificate. In a Certificate Chain, a higher placed Certification Authority approves a lower placed Certification Authority by signing their Certificate. The Certificate of the highest placed CA (Root CA) is self-signed.

PKI Disclosure Statement (PDS): A document that complements a CP or a Certificate Practice Statement that contains the fundamental information regarding a CA's policies and practices. In a PKI Disclosure Statement, information that is usually recorded in detail in a CP or a CPS can be brought up and highlighted. A PKI Disclosure Statement does not replace either one, but is instead their summary.

Certification Practice Statement (CPS): A description of the CA's technical and functional envinronment and the division of responsibilities and obligations between parties. A CPS adheres to principles described in the CP.

Certificate Policy (CP): A description of the principles governing Certificate issuance and the responsibilities of the parties relying in the Certificates.

Certificate Profile: A detailed description of a Certificate's technical parameters.

Certificate Generation: A process that produces Certificates and maintains their revocation information.

Certification Authority (CA): An organization that issues Certificates. CA is responsible, among other things, for generating Certificates and creating the CP and CPS describing its activities.

CA Private Key: The private key that a CA uses for issuing Certificates and signing CRLs they have published.

CA Key Backup: An arrangement that guarantees possibility to restore a CA's Private Key if it is destroyed.

Certificate Rekey: A situation wherein a Certificate is renewed so that the Keypair changes but the Certificate's identity remains the same. The validity period of the Certificate may change.

Certificate Subject: The party that uses a private key associated with a Certificate. A Certificate's subject-field identifies the Certificate subject. The subject can, for example, be a specific service or a business organization.

Subscriber: Party that requests for a Certificate and who is responsible for the issued Certificate. A Subscriber company usually has a representative who requests for the Certificate on its behalf.

Subscriber's agreement, in CA context: An agreement between a Certificate Subscriber and a CA that defines the rights and responsibilities of the parties with regard to Certificate issuance and management.

Certficate Suspension: Adding a Certificate temporarily to the CRL.

Certificate Modification: A situation wherein a Certificate's information content changes but the Key Pair and validity period remain the same.

Certificate Revocation: Permanent invalidation of a Certificate by adding it to the CRL.

Certificate Renewal: A situation wherein a Certificate is renewed but the Key Pair and the Certificate's information content remain the same. The Certificate's validity period may change.

Private Key: The private part of the Key Pair used in Public Key Infrastructure for asymmetric encryption. This key has been designated unambiguously to a specific party, therefore enabling it to be used for, for example, creating a Digital Signature. Data encrypted using the Keypair's public key can be decrypted using the Private Key. In addition, it can be used for establishing a shared secret. In certain Public Key algorithms, data encrypted using the Private Key can be decrypted using the Keypair's Public Key. Such algorithms include RSA, that is used by this CA.

X.509: The most commonly used ITU (International Telecommunication Union) –standard for Public Key Infrastructure (PKI). In X.509, the standard format of Public Key Certificates, CRLs, attribute Certificates and Certificate's Certificate chains' is defined. X.509 is ITU's recommendation, which is why PKI vendor's have implemented standards in various ways.

3.2 Abbreviations

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List

ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module, Physical security device for protecting private keys
ITU	International Telecommunication Union
NCP	Normalized CP
OCSP	Online Certificate Status Protocol, a service that returns current Certificate status information
OID	Object Identifier, A unique identifier
PDS	PKI Disclosure Statement, summary of CP
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivest Shamir Adleman, a widely adopted public key encryption algorithm

3.3 Notation

Not in use.

4 GENERAL CONCEPTS

The CA operates as the users' (Relying Parties) trusted third party for Certificate generation, issuance and use-related matters. The CA is marked as the issuer of such Certificates that have been signed with the CA's private key. The CA is responsible for its possible subcontractors' activities as for its own.

4.1 Certification Authority (CA)

OP Cooperative acts as this Root CP's Root CA (hereafter Root CA). Within this document, the term CA is used to refer to both Root CA and Subordinate CA.

CA's tasks include:

1. CA's Certificate Service's management.
2. Implementation and management of the Registration Service associated with the CA's Certificate Service.
3. Certify the Public Keys of the Subordinate Certificates that CA has approved.
4. Ensure that the CA's services described in this document are available for use of the Relying Parties.

4.2 Certification Services

Certificate Services include the following services:

1. Registration services: Identifying Certificate Subscriber or their representative and validating their authorization.

2. Certificate Generation services: Certificate generation and signing based on the identity that was authenticated at the Registration services along with other confirmed Subscriber details.

3. Revocation service: Handling Revocation Requests and related reports as well as making decisions on necessary actions.

4. Validation Authority service: Notification of revoked Certificates to Relying Parties. The notification service can be continuous or the information can be delivered or published at agreed upon intervals.

4.3 Certificate Policy and Certification practice statement

4.3.1 Purpose

Generally speaking, CP answers the question ”What?” where CPS answers the question ”How?”.

CP defines the requirements and standards necessitated by PKI activities for different areas. CPS, on the other hand, tells what kind of practices and controls the CA and other parties need apply to fulfill the requirements set in the CP. Therefore, the purpose of CPS is to describe how different parties perform their operations and control their processes.

4.3.2 Level of specificity

CP describes the general requirements for the CA’s activities. CP, on the other hand, records in more detail the functions with which the CP’s requirements are fulfilled.

4.3.3 Approach

CP is not tied to a certain technology or model. Its purpose is to be general and lay a foundation for a trustworthy PKI system.

CPS, on the other hand, is a more detailed description and it is therefore tied to a certain target.

4.3.4 Other CA statements

In addition to CP and CPS, the CA can also publish other PKI-related documentation, such as PKI Disclosure Statement, Certificate Subscriber’s Agreement, Relying Party Agreement etc.

4.4 Certificate Subscriber and Certificate Subject

In this document two different terms are used to distinguish between two Certificate-related roles:

1. Certificate Subscriber is the responsible party that requests for a Certificate from the CA.

2. Certificate Subject is the party identified in the Certificate.

In the Registration the Subscribing organization is represented by a person authorized by the organization.

Under this policy, the Certificate Subject can be a unit or a function producing or managing OP-Group’s business or ICT services or another party approved by Root CA. The Certificate Subject uses the Private Key on behalf and responsibility of Certificate Subscriber.

5 INTRODUCTION TO CERTIFICATE POLICIES

5.1 Overview

CP is a group of rules that indicate a Certificate's suitability for a named community and define the associated shared information security requirements. Certificates issued under this CP contain identification information with which Relying Parties can assess the Certificate's suitability and trustworthiness for the required use.

5.2 Identification

This CP is used only in connection with services offered or authorized by OP-Group. As the most authoritative document of the Certificate Chain this Certificate Policy is the foundation for the service's legal and technical requirements.

This CP's identifier (OID) is 1.3.6.1.4.1.11374.1.1.1.1.3.

5.3 Certificates' usage purposes

Certificates issued by this CA are used as Subordinate Certificates in OP- Group services.

Certificates issued by Root CA are also used for other purposes separately specified by Root CA.

Using the Certificates for other purposes is prohibited.

OP-Pohjola Root CA is marked as the Certificate issuer.

5.4 Conformance

5.4.1 General

The CA produces Certificate Service with the conditions mentioned in the Certification Policy and is answerable to the Certificate Subject for the Certificate Service's functionality. The CA is responsible for the entire Certificate system's functionality, also on the part of the possible subcontractors it uses.

The service's compliance can be verified by comparing the policy to practice during the CA's activities as well as after major process or documentation changes.

5.4.2 Requirements

CA fulfills the obligations described in chapter 6 and adheres to the practices defined in chapter 7. All parties connected to this Root Certificate must adhere to this Certificatee Policy.

5.4.3 Other conditions

Translations can be made of this document to other languages. If conflicts arise between the translations and the document in Finnish, the Finnish version prevails.

6 RESPONSIBILITIES AND OBLIGATIONS

6.1 Root CA's obligations

1. It is Root CA's responsibility take care that all requirements set in chapter 7 are executed according to this CP.

2. It is Root CA's responsibility to ensure that all Certificate services offered by it conform to the valid CPS.

6.2 Subordinate CA's obligations

Subordinate Certificate's Subscriber and Subject can be the same entity. Certificate Subscriber is responsible also for the Certificate Subject's obligations. Root CA binds Subordinate CA with an agreement to conform to the following conditions:

1. Compliance with this policy: Subordinate CA is responsible for taking care that all requirements set in chapter 7 have been implemented according to the CP.

2. Correct and complete information: Subordinate CA is responsible for delivering correct and complete information along with the certificate signing request.

3. Diligence: Subordinate Certificate's Subject is obligated to handle their Private Key diligently in order to prevent misconduct.

4. Certificate Subject's keys' length: Subordinate CA's responsibility is to select keys' lengths so that they are sufficient for the Certificate's usage purposes defined in this CP for the duration of its validity.

5. Key generation: Subordinate CA is obligated to create its Key Pair using an algorithm that is commonly (for example, according to standard NIST SP800-57) seen as strong enough for the Certificate usage purposes defined in this CP. Subordinate Certification Authority is obligated to create the keys in a HSM device validated at least to level 3 of standard FIPS PUB 140-2.

6. Key access control: Only a party authorized by the CA Certificate Subject has a right to use the CA's Private Key. The key is stored and used in an HSM device dedicated for the use of OP Cooperative's Subordinate Certification Authorities.

7. Notification requirement: if one of the following occurs or is suspected to have occurred prior to CA Certificate expiration, Subordinate CA is obligated to inform Root CA of it without delay:

    i. Certificate Subject's Private Key goes missing, is stolen or its integrity is compromised.

    ii. Control of the Certificate Subject's Private key is lost, for example if administration cards go missing.

    iii. A fault or a need for change is noticed in Certificate content.

    iv. Certificate issuance prerequisites have changed.

8. CA key compromise: Subordinate CA is obligated to immediately remove from use the compromised Subordinate Certificate Subject's Private Key and all Certificates based on it and to deliver Subordinate CA Certificate's revocation request to Root CA.

9. Subordinate CA is obligated to conform to this CP, Root CA's CPS, its own CP, and its own CPS. If conflict arises, this CP prevails.

10. Subordinate CA is responsible for conforming to Finnish legislation in force and applicable to its industry.

11. Subordinate CA is obligated to update its own CP and CPS without delay, if such changes take place in Subordinate CA's activities that necessitate changing the said documents or if Root CA's CP or CPS undergoes such changes that necessitate the changing of Subordinate CA's equivalent documents.

12. Subordinate CA is obligated to include the Relying Party obligations described in section 6.3 into its Certificate Subscriber's agreements.

13. Subordinate CA is obligated to store essential information related to Certificates for at least 10 years from the time of occurence.

14. Subordinate CA is obligated to publish its name and contact information in a manner that ensures their availability to Relying Parties.

6.3 Relying Party obligations

By trusting in the Certificate, the Relying Party expresses its acceptance of the conditions of this CP.

Relying Party is obligated to confirm the following for the entire Certificate Chain:

1. Inspect the Certificate's validity and possible revocations or suspensions from Validation Authority and confirm the validity and integrity of the revocation information.
2. Adhere to the Certificate use limitations set in the Certificate or conditions for Relying Parties.
3. Adhere to all precautions mentioned in the agreements or other Certificate-related documents.
4. Accept the Certificate only for the usage purposes specified in the CP. In addition, the Relying Party must assess whether the CA's trust level described in the CP is sufficient for the purposes of the Relying Party.

6.4 Root CA's responsibilities

1. Root CA is responsible for adhering to the procedures and practices described in this CP in its Certificate Services, unless not adhering to them is due to force majeure.
2. Root CA is responsible for adhering to current Finnish legislation.
3. Root CA is responsible for identifying Subordinate Authorities and confirming authorization.
4. Root CA, in addition to its own activities, is responsible for ensuring that all parties participating in the production of the Root Certification Service act in accordance with this CP.
5. Root CA is responsible for ensuring that Subordinate Certification Authorities' Certificate Policies and CPSs approved by it are compliant with this CP.
6. Root CA is in no way responsible for damages caused by the use of Certificates issued by a Subordinate CA, unless the damages are caused by Root CA acting in violation of this CP.
7. Root CA is not responsible for the use of Certificates issued under this CP or the associated keys, when they are used in a way that violates this CP.
8. Root CA is not responsible for the use of trademarks in Certificates issued by Subordinate Certification Authorities.

6.5 Subordinate CA's responsibilities

Root CA issues subordinate Certificates only to Subordinate Certification Authorities that have committed contractually to the following responsibilities:

1. Subordinate CA is responsible for adhering to this CP and its own current CP and CPS.
2. Subordinate CA is responsible for ensuring its Private Key is used only for the purposes defined in Subordinate CA's CP. The defined usage purposes may be signing a Subscriber's Certificate, issuing an OCSP Certificate, signing a CRL and other CA's signing purposes, such as signing CA's audit log data.
3. Subordinate CA is responsible for identifying the Subscribers of the Certificates it has issued and confirming their authorization.

4. Subordinate CA is responsible for ensuring that it owns or has the right to use the names and trademarks it uses, that are mentioned in the subordinate certificate request or the Certificate's information fields.

6.6 Relying Party responsibilities

By trusting in the Certificate, the Relying Party acknowledges its acceptance of the CP conditions.

The Relying Party is responsible for any other tasks required for authorizing or approving an event in addition to verifying the Certificate.

7 REQUIREMENTS ON CA PRACTICE

In this chapter, Root CA's activities are described and requirements are set for Subordinate CA's activities, unless otherwise stated.

7.1 Certification practice statement (CPS)

Control objective: CA describes its practices and procedures in the CPS.

1. CA has a CPS to which the practices and procedures are defined with which the requirements set in the CP are fulfilled.

2. CPS describes the responsibilities and practices of the parties involved in Certificate production.

3. CA separately decides on publishing the CPS.

4. CA approves the CP and CPS.

5. CA reviews the CPS at minimum at two year intervals and decides on required actions, such as performing of audits.

7.2 PKI key management life cycle

7.2.1 Generation and management of CA keys

Control objective: Certificate generation and management – CA confirms that the keys for the CA's Certificate are created in controlled conditions according to instructions created beforehand and approved by the CA.

1. CA keys are generated in a physically secure space (see section 7.4.4). Key generation is handled by appropriate persons (see section 7.4.3) under Dual Control. More detailed practices have been described in CPS.

2. CA key generation is executed using an HSM device that fulfills the requirements set in section 6.2 step 5.

3. Root CA is a so-called offline CA, which means that its technical environment does not include network connections outside it. All operations performed within this environment are manual.

4. CA key generation is performed using an algorithm that is commonly seen as strong enough for the purposes of a CA. Key parameters, especially the key length are selected so that they are strong enough for the CA's signing purpose. Algorithms, key lengths and other parameters are compliant with standard NIST SP800-57 or newer applicable recommendations. More detailed descriptions can be found in the CPS.

5. Personnel participating in the CA's key operations have been listed and named, trusted roles have been assigned to them (see section 7.4.3) and all key operation tasks are always

performed under Dual Control. Functions related to the CA's Private Key or its device environment are always recorded in a log.

6. When a person ceases to act in a trusted role, their access rights associated with the trusted role are immediately removed and smart cards related to the key operations are passed onto the next role holder.

7. Before the CA's Private Key expires, the CA creates a new Certificate Key Pair. The new CA Certificate's distribution procedure does not differ from the old Certificate's distribution procedure. This guarantees undisturbed continuity of functions depending on the CA's Certificate. A new Keypair is created and the new Public Key is distributed according to this CP.

7.2.2 CA key storage, backup and recovery

Control objective: CA ensures that its private keys retain their confidentiality and integrity thoughout their life cycle.

1. CA's Private Key is protected using an HSM device. Root CA's Private Key is protected using an HSM device dedicated only for the use of OP-Cooperative's Root Certification Authorities.

2. Root CA's Private Key backing up, storing and recovery can only be performed by named persons (see section 7.4.3) in a physically secure environment (see section 7.4.4) so that at least two persons named and authorized for the task are always present.

3. CA's Private Key backups are protected using the same procedure that is used for the key in production use.

4. The procedures have been described in more detail in the CPS.

7.2.3 CA Public Key distribution

Control objective: CA ensures that its Public Key retains its integrity and authenticity as it is transfered or distributed to Relying Parties for their use.

Root CA's Certificate is published at address: https://www.op.fi/varmennepalvelu. The page is protected using an organization validated service Certificate. The Certificate's fingerprint and serial number are also published on the same web service.

7.2.4 Key escrow

Key escrow is not in use for Certification Authorities' keys.

7.2.5 CA key usage

Control objective: CA ensures that the CA's Private Keys are used appropriately.

1. Root CA's Private Key is used both for signing Root CA's Certificate as well as signing Subordinate Certificates (see section 7.3.3) and CRLs needed by OP Group. Root CA's Private Key is not used for any other purpose.

2. Root CA's key is activated by at least two persons named for a trusted role, who remain present as long as Root CA's Key is active.

7.2.6 End of Root CA key life cycle

Control objective: Root CA ensures that its Private Keys are not used after their life cycle ends.

All copies of the the CA's Private Key are destroyed or removed from use without delay once their expiration date passes. This prevents their use for the purposes listed in section 7.2.5 after expiration.

7.2.7 Life cycle management of HSM device

Control objective: CA ensures its HSM devices' integrity for the entire duration of their life cycle.

1. CA's HSM devices are protected from unauthorized handling during their transportation. At least two named and authorized persons inspect the HSM device during its installation. In the inspection the inspecting persons establish that the HSM device has not been handled without authorization during the transportation and that it fulfills the security standards (See section 7.2.2).

2. The HSM device is protected from unauthorized handling during storage.

3. At least two authorized persons are required for the HSM device's deployment, initialization, and use.

4. When the HSM device is removed from use, it is destroyed or erased according to manufacturer instructions.

7.2.8 CA provided subject key management services

Control objective: CA has exclusive control of its Private Keyf.

1. Subordinate Certification Authority itself creates the Subordinate Certificate's Key Pair.

2. Certificate request is delivered to Root CA for signing using a manual procedure

3. Subordinate CA's Private Key always remains under the control of Subordinate CA, protected by the HSM device.

7.3 PKI Certificate life cycle management

7.3.1 Subordinate CA Certificate registration

Control objective: Root CA confirms that the Subordinate Certificate Subscriber's name and other details have been provided correctly. In addition, Root CA confirms that certificate requests are correct, authorized, appropriate and thorough.

1. CA approves only Finnish OP Group communities as Subordinate CAs.

2. Certificate Subscriber commits to adhering to this CP as a part of the registration. Certificate Subscriber accepts the Subscriber's agreement and possible other related agreements.

3. Root CA validates the Subordinate Certificate Subscriber's identity and authorization to act on behalf of Subordinate CA.

4. Subordinate CA delivers its CP and CPS to Root CA that validates that they are not in conflict with this CP or Root CA's CPS. It is recommended that Subordinate Certification Authorities adhere to the same standards and structure in their Certificate Policies as Root CA.

5. Root CA decides whether to accept or reject subordinate certificate requests.

6. Root CA archives the agreement signed with the representative of the Subordinate Certificate Subscriber.

7. Root CA stores the registration information for ten years after Root CA's activities end.

8. Subordinate Certification Authority's technical certificate signing request is created and transferred to Root CA in a manner defined by Root CA. In the delivery of the technical certificate signing request, the integrity of the Certificate request is ensured from the moment of its creation to Certificate Generation.

9. Root CA verifies that the Subordinate CA has in its possession a Private Key that matches the certificate request and that the certificate request has been delivered by Subordinate CA.

7.3.2 Certificate renewal, rekey and update

Control objective: Subordinate CA's new Subordinate Certificates are handled identically to new CA subscriptions. Root CA additionally ensures that Certificates are not issued for keys that were used earlier.

1. Certificate renewal requests are always handled as new Certificate subcriptions.
2. Root CA can issue a new Subordinate Certificate under the existing Subscriber's Agreement.
3. Root CA does not issue a Certificate for a Key Pair in use, but instead always requires generation of a new Key Pair.

7.3.3 Certificate generation

Control objective: Root CA ensures that Root CA and Subordinate CA Certificates' issuing process are secure so that the integrity of the Certificates is retained.

Certification Authorities' keys are always generated in secure conditions under Dual Control, adhering to the requirements provided in section 7.2.1.

7.3.3.1 Root CA Certificate generation:

1. Root Certificates' contents have been covered in detail in the CPS.
2. Root Certificate's validity period is 29 years.
3. Root CA Certificate is signed in connection with Root CA key generation.

7.3.3.2 Subordinate CA Certificate generation:

1. Subordinate Certificate content requirements are covered in detail in Root CA's CPS.
2. Subordinate Certificates' validity period is at most 7 years.
3. Root CA ensures that during its existence it issues only unique serial numbers to Subordinate CA Certificates.
4. In Subordinate CA Certificates, such names to describe the CA are used that Relying Parties can identify the party acting as Subordinate CA.
5. Subordinate CA Certificate is created in a separate, Root CA-approved Certificate Generation Ceremony.

7.3.4 Distribution of terms and conditions

Control objective: CA ensures that Certificates' terms and conditions are available to Certificate Subscribers, Certificate Subjects and Relying Parties.

CA higher in the Certificate Chain delivers its Certification Practice Statement to its Subordinate CA.

Certification Authorities' Certificate Policies are published at address: https://www.op.fi/varmennepalvelu.

Subscriber's Agreements must be available to Subscribers.

7.3.5 Certificate dissemination

Control objective: CA ensures its Certificate's availability to Relying Parties.

1. When Subordinate CA's Certificate has been generated, its integrity is checked prior to its delivery to the Certificate Subscriber and Certificate Subject.
2. Subordinate CA is responsible for the distribution of its Certificate.
3. Root Certificate is available as stated in section 7.2.3.

7.3.6 Certificate Revocation and Suspension

Control objective: Certificates are revoked in timely manner based on authorized and validated Certificate Revocation Requests.

7.3.6.1 Certificate Revocation management

1. Subordinate CA Certificate Revocation Request can only be made by Subordinate CA's Representative or Root CA.
2. Subordinate Certificate Revocation Requests are delivered to Root CA.
3. Revocation information is available to all Relying Parties in the Revocation Information Service as described in the CPS.
4. Subordinate CA Certificate can be revoked, for example, in the following circumstances:
    i. Subordinate Certificate's Private Key is compromised.
    ii. Subordinate Certificate Subscriber's Agreement or its obligations are violated.
5. Revocation Requests are handled without delay.
6. Revocation Requests are authenticated according to CPS.
7. When a Certificate has been permanently revoked, it can no longer be returned back to use.

7.3.6.2 Revocation information

1. When using CRLs to convey revocation information:
    i. Root CA CRL's validity time is one year and it is published at least two times a year.
    ii. Each CRL states its validity time.
    iii. A new CRL can be published before the scheduled publishing time.
    iv. CRL is signed by the CA.
2. Revocation information can also be published as a realtime service (OCSP).
3. Revocation information is available continuously while the Root Certificate remains valid.
4. Revocation Information contains status information of revoked certificates at least for the duration of their original validity period.

7.4 CA management and operation

7.4.1 Security management

Control objective: CA confirms that applied administrative and management practices are adequate and standards-compliant.

1. CA performs risk assessments on its activities and defines the needed security requirements and practices.

2. CA is responsible for its possible subcontractors' activities as for its own.

3. CA operates according to predetermined practices in order to ensure quality and information security in production of the certificate service.

4. CA actively maintains its certificate production environment, specifically paying attention to information security and requirements pertaining to it.

5. Security controls and procedures in the CA certificate service's premises, systems, and information repositories are documented and maintained. Rules, instructions and processes regarding the Certificate Service's production are documented and approved. In addition, the CA has a recovery and continuity plan in order to be prepared for incidents, accidents and the like.

7.4.2 Information classification and management

Control objective: CA handles its datasets and information properly.

CA has in its use practices and guidelines for document and information classification, handling and destruction.

7.4.3 Personnel security

Control objective: CA ensures that its personnel policy contributes to and supports the trustworthiness of the CA's activities.

7.4.3.1 General matters pertaining to personnel security

1. CA has in its use a sufficient number of personnel with the required expertise, experience and qualifications for the services provided as well as their tasks.

2. OP Group has determined the trustworthiness and suitability of the personnel for their tasks using normal recruitment practices.

3. With regard to subcontractors, their trustworthiness and suitability for their tasks is ensured contractually.

4. CA's trusted roles are described unambiguously.

5. CA's personnel (both temporary and permanent) have defined job descriptions that adhere to principles of segregation of duties as well as least privilege.

7.4.3.2 Registration, Certificate generation, Certificate Revocation management

1. The personnel managing the CA have experience and training in PKI techniques and they have acquainted themselves with personnel security practices in tasks that entail security responsibilities. In addition, they have sufficient experience in information security and risk assessment.

2. Personnel members carrying out CA's trusted tasks must have no conflicts of interest that may affect the trustworthiness of the CA's activities.

3. Trusted roles are defined in the CPS.

4. No person convicted for a serious crime or such offence that affects their suitability for the task is accepted to trusted roles or managerial positions. Personnel have no access to trusted tasks before the required background checks have been completed. Background checks are performed within the constraints of laws and official regulations.

7.4.4 Physical and environmental security

Control objective: CA ensures that physical access to critical assets is controlled and that physical risks related to CA's assets are minimized.

7.4.4.1 General matters pertaining to physical security

1. Only properly authorized persons are allowed access to spaces where procedures associated with Root or Subordinate Certificate Generation or revocation are performed.

2. CA defines controls with which accidents, damages, risk to property and theft of or danger to data or production facilities are prevented.

3. Dual Control is used in all operations related to Root CA's equipment.

   i. When the device is in storage, the storage space access control is under Dual Control.

   ii. The device is operated under controlled conditions in a dedicated location.

4. All operations associated with CA equipment are documented.

7.4.4.2 Certificate production and revocation event management

1. Workspaces where Certificate Generation or revocation management-related tasks are performed have been physically secured so that no unauthorized access to the systems or data can take place.

2. In the physically secured area, external persons are escorted and are never left unmonitored by an authorized person.

3. To ensure physical security, CA has an area secured using access control for Certificate Generation and Revocation management-related tasks.

4. CA's physical security and perimeter security practices cover physical access control, natural disaster preparation, fire safety factors, support system malfunctions, building collapses , water and other pipe damages, preparation for theft, break-ins and recovery plans.

5. To secure CA's devices, data, communication equipment and software, controls are in place to prevent their unauthorized seizure. In the same secure area, other operations can also take place with the assumption that only authorized personnel are allowed to enter the area.

7.4.5 Opearations management

Control objective: CA ensures that its systems are secure and that they are operated correctly, minimizing risk of failure.

7.4.5.1 General matters pertaining to operations management

1. CA secures the certificate systems' integrity and data against viruses, malware and unauthorized software.

2. CA minimizes damages caused by information security breaches and malfunctions by using incident notification practices and action plans.

3. CA handles the storage devices it uses securely to protect them from damage, theft and unauthorized use.

4. CA uses storage device management practices that prevent storage device lifepan running out or deterioration during document storage.

5. CA defines formal practices that apply to all trusted and managerial tasks associated with providing certificate services.

7.4.5.2 Storage device handling and security

All storage devices are handled securely and adhering to requirements based on information classification (see 7.4.2). When no longer used, storage devices containing sensitive information are destroyed securely.

7.4.5.3 Reacting to and notifying of deviations

1. Persons participating in CA's activities notify of all deviations as soon as possible after the event to CA. CA reacts to deviations in a quick and coordinated manner to limit the effects of the deviations.

2. Audit log processes in adherence with section 7.4.11 function from system startup to shutdown. In terms of physical monitoring of the HSM device, audit log processes function also when the device is in storage.

7.4.6 System access management

Control objective: CA ensures that only authorized persons have access to CA's systems.

7.4.6.1 General matters pertaining to systems' access control

1. CA's user and authorization management practices restrict system access based on work task. CA ensures that access to system data and functions is restricted according to access management policy.

2. CA's personnel are identified reliably before credentials to access applications critical to Certificate management are handed over to them.

3. CA's personnel are responsible for the operations they perform. This is supported by event log retention. (ks. luku 7.4.11).

7.4.6.2 Certificate generation

1. Root CA ensures that the devices it uses in its certificate production are in no point connected to any network.

2. Devices' configuration is documented and it is verifiable in connection with general auditing.

7.4.6.3 Revocation information

Revocation information system falls under the the access management scope.

7.4.7 Trustworthy systems deployment and maintenance

Control objective: CA uses trustworthy systems and products that have been protected against unauthorized modification.

7.4.7.1 General matters pertaining to trusworthy systems

1. In each CA system development project, the system's security requirements are analyzed in the system planning and requirement specification phase. Security solutions implemented based on the analysis are used to ensure that security is built-in to the systems.

2. Change management processes exist for deployments, modifications and emergency updates that apply to operative applications.

7.4.8 Business continuity management and incident handling

Control objective: CA ensures that in catastrophe situations, such as in the event of CA private key compromise, operations return to normal as quickly as possible. Other emergency situations include device or software components' critical errors.

7.4.8.1 General matters pertaining to continuity

CA has a regularly updated continuity plan to prepare for catastrophe situations.

7.4.8.2 Backup and restoration of CA systems

CA has sufficient backup systems to ensure that in catastrophe situations or upon system malfunction all essential business information and software can be restored.

7.4.8.3 CA key compromise

CA's business continuity plan (or recovery plan) covers CA's private key compromises or presumed compromises and an action plan exists to address them.

Upon CA key compromise, the following actions are taken:

1. Notify all Certificate Subscribers and other parties with whom the CA has agreements or other established connections, such as Relying Parties or other Certification Authorities, of what has taken place.

2. Notify the aforementioned parties that Certificates and revocation information, in the issuance of which the now compromised key was used, are no longer viable.

7.4.8.4 Algorithm compromise

If one of the algorithms used by the CA, or an associated parameter, turns out to be too weak for its usage purpose, the CA

1. Notifies of the matter all Certificate Subscribers and Relying Parties, with whom the CA has agreements or other established connections.

2. Relying on its own judgement, revokes all Certificates affected by the compromise.

7.4.9 CA termination

Control objective: When the CA's activities are shut down, retaining the confidentiality of the CA's key is ensured. In addition, CA ensures that maintenance of records needed for possible future investigations by authorities or legal proceeding continues.

CA performs at minimum the following actions prior to shutting down of its activities:

1. CA notifies the following parties of shutting down of its activities: all Certificate Subscribers and Relying Parties with whom the CA has agreements or other established connections. In addition, other Relying Parties are notified of the shutting down of activities.

2. CA cancels all of its Subcontractors' authorizations to act on behalf of the CA in functions related to Certificate issuance.

3. CA performs all of the needed actions in order to transfer the responsibility of the registration information maintenance (see 7.3.1), Revocation information service (see. 7.3.6) and event log archiving (see 7.4.11) and to ensure their availability to Certificate Subscribers and Relying Parties for as long as it was originally stated.

4. CA destroys or removes from use its Private Key as defined in section 7.2.6.

7.4.10 Compliance with legal requirements

Control objective: CA ensures that its activities are in adherence with the current Finnish legislation.

Finnish law is applied to this CP and Root CA's activies, omitting its conflict of laws provisions.

7.4.11 Information retention

Control objective: CA ensures that all essential information related to Certificates is stored for the appropriate period.

Certificate-related files include registration information (see 7.3.1) and event information related to CA's environment, key management and Certificate Management.

7.4.11.1 General matters pertaining to information storage

CA

1. Maintains the confidentiality and integrity of files related to Certificates

2. Ensures that files related to Certificates are complete and dependably archived

3. Ensures the availability of files related to Certificates, if they contain information necessary for possible legal actions.

4. Records the accurate time of management events of CA's environment, keys and Certificates.

5. Stores Root Certificate-related files at minimum for 10 years from the time when Root CA's activities are shut down.

6. Records events in a log so that log data cannot be modified or destroyed without authorization.

7. Describes the events to be documented on a general level in the CPS

8. Ensures the archives' availability and readability even in the case where CA's activities are interrupted or shut down.

9. Protects log and archive data from unauthorized viewing, modification and deletion and stores all backups separate from the Certificate system environment in a location with at least the same security level and tests their usability.

7.4.11.2 CA

CA stores the following information regarding its activities:

1. Agreements and service descriptions addressing the Certificate Service.

2. Audit reports and minutes that contain the information of the auditing of the CA's activities.

3. Current and earlier published Certificate Policies.

4. Audit trail of CA's activities.

7.4.11.3 Certificate production

CA records the following information regarding procedures concerning the Certificate system:

1. CA's private key generation and renewal-related events, including keys' information.
2. User account creation.
3. Procedure requests and the associated account information, request type, information on whether the procedure was completed or not and reason for possible interruption.
4. Installation of new software or update of existing software.
5. Backups' dates, times and other information.
6. System halt and restart information.
7. Date and time of all device upgrades.
8. Log data creation date and time.

7.4.11.4 Registration

CA ensures that all events related to registration are recorded in a log.

7.4.11.5 Certificate generation

1. CA records in a log all events related to CA Keys' life cycle.
2. CA records in a log all events related to Certificates' life cycle.
3. CA also records in a log all events related to the HSM device.

7.4.11.6 Revocation service management

CA ensures that all requests and reports related to the Revocation Service and operations following them are recorded in a log.

7.5 Document management

This CP is owned and maintained by OP Cooperative.

7.5.1 Change management

This document is reviewed at least every two years. The document can be updated, and depending on the nature of the changes, all Relying Parties are notified of them as follows:

Minor changes that do not require a notification:

- Document appearance changes
- Grammar fixes are done in the document
- A translation of the document is done.

Changes that affect the actual content, that require a notification::

- Contact person, other mentioned contact details or informative web addresses change

- Changes affecting agreements between parties are notified of according to the agreement terms in question

- Any part of the CP can be changed by bringing the change to the knowledge of all Relying Parties at least 60 days prior to the change entering into force.

Root CA notifies of changes directy to Subordinate Certificate Authorities.

Root CA can, with a unilateral decision, replace this policy with a new policy.

7.5.2 Version management

Root CA archives all published and approved Certificate Policies.

Version	Date	Changes
1.0	6.2.2013	First approved and published version.
2.0	15.9.2014	Updated and changes approved
2.1	5.12.2016	Implemented changes based on review of Finnish language version.
3.0	6.3.2017	Updated in 2016. Approved to be published.

7.5.3 Contact details

Questions regarding the CP are answered by Root CA’s contact person.

Postal address: OP / Jukka Ikäheimonen, PL 909, 00101 Helsinki

Phone: 010 252 010 (Jukka Ikäheimonen)