OP-SERVICES LTD
CERTIFICATE POLICY

OP WS CA

Version 2.0
Valid from 6.3.2017

OID: 1.3.6.1.4.1.11374.1.2.1.1.1

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.

This CP is a set of rules drawn up by OP-Services Ltd for implementing Certificate Service and issuing Certificates for the use of OP Financial Group's Web Services channel.

Identification information:

OP-Services Ltd, Certificate Policy, OP WS CA, version 2.0

OID: 1.3.6.1.4.1.11374.1.2.1.1.1

1 SCOPE

This CP applies to OP Financial Group's CA OP WS CA (hereafter CA). In addition, the CP is applied to actions concerning life cycle management of the Certificates issued by this CA. The CP defines the obligations and responsibilities of the CA, Subscribers, Relying Parties as well as other actors related to the Certificates.

OP WS CA issues Certificates to End-entities of OP Financial Group's Web Services Channel (hereafter WS Channel). Using the issued Certificates the End-entities can sign service requests forwarded through the Web Services Channel.

This CA is OP-Pohjola Root CA's (hereafter Root CA) Subordinate CA. In the operations of OP WS CA, the principles, responsibilities and obligations defined in Root CA's CP are adhered to.

The Relying Parties must always check before accepting a Certificate that OP WS CA-issued Certificates' CA chain reaches the Root CA defined in this CP or another Root CA above it approved by OP Financial Group. The Root CA defined in this CP must nevertheless always be a part of the certificate hierarchy. Otherwise, the Relying Parties must reject the Certificate.

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
NIST SP800-57	NIST Special Publication 800-57: Recommendation for Key Management
Root Certificate Policy	OP Financial Group, Business Services' Root Certificate Policy OID: 1.3.6.1.4.1.11374.1.1.1.1.3

3 DEFINITIONS, ABBREVIATIONS AND NOTATION

3.1 Definitions

Audit trail: Requirement for log entries to be made in a manner that enables accurate traceability of actions performed in a system.

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

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

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.

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 certificatation authority accredits a lower placed Certification Authority by signing their Certificate. The Certificate of the highest placed CA (Root CA) is self-signed.

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

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

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

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

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

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

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

Certificate Suspension: Adding a Certificate temporarily to the CRL.

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.

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

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.

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.

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.

End-entity: In this context: Party that has made an agreement for the use of certificate services and has signed the Subscriber Agreement.

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

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.

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.

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

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.

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.

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.

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 Key Pair'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.

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: 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.

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.

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

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.

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. The Relying parties include, for example, Certificate subjects, business services using OP Financial Group's Certificates or other third parties.

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

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.

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.

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).

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: see Certificate Subscriber.

Subscriber 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.

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.

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 creation, 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 CA

OP-Services Ltd acts as a CA in adherence with this CP. CA's tasks include:

1. Governing OP-Services Ltd's WS-channel's CA.
2. Implementation and management of the Registration Service associated with the CA's Certificate Service.
3. Certify the Public Keys of the End-entities and services it 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. OP Financial Group member banks' branches act as RA points and bank employees as RAs.

2. Certificate Production services: Certificate creation and signing based on the identity that was authenticated at the Registration Services and other attributes. OP-Services Ltd produces the Certificate production services.

3. Revocation service: Handling Revocation Requests and related reports as well as making decisions on necessary actions. The Revocation Service is operated by OP Financial Group member bank branches during their opening hours and the 24/7 telephone service (see section 7.5.3).

4. Validation Authority: Notification of revoked Certificates to Relying Parties. VA is implemented in form of a CRL that is published regularly. The CA can also offer a real-time certificate status information request service (OCSP).

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 to implement 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

The CP describes the general requirements for the CA’s operations, while the CPS, 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 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.

The Certificate Subject uses the Private Key on behalf and responsibility of the Subscriber. Every Certificate Subject is uniquely named. No such information is derivable from the name that would uniquely identify the Certificate Subject to parties outside OP Financial Group.

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 Financial Group.

This CP adheres to OP Financial Group's Root CA's CP.

This CP's identifier (OID) is 1.3.6.1.4.1.11374.1.2.1.1.1.

The Root CA's CP's identifier (OID) is 1.3.6.1.4.1.11374.1.1.1.1.3.

5.3 Certificates' usage purposes

The Certificates issued in adherence with this CP can be used to verify data origin and integrity in interaction between the WS-channel and its End-entities. OP WS CA can issue Certificates also for signing OCSP responses.

Using the Certificates for other purposes is prohibited.

OP-Pohjola WS CA or OP WS CA V2 is marked as the Certificate issuer. The CA name's version number is incremented in connection with CA Certificate re-key. OP Pohjola WS CA name is replaced with OP WS CA V2 name upon the first re-key.

5.4 Conformance

5.4.1 General

The CA produces Certificate Service with the terms 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 the CA Certificate described in this document must adhere to this CP and OP Financial Group Root CA's CP.

5.4.3 Other terms

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 CA's obligations

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

2. It is the CA's responsibility to ensure that all Certificate services offered by it (see section 4.2) conform to the valid CPS.

3. The CA is obligated to obtain Root CA's approval for its own CP and CPS and update them without delay, if such changes take place in the CA's activities that necessitate changing the said documents or if the Root CA's CP or CPS undergoes such changes that necessitate changing of the CA's equivalent procedures or documents.

6.2 Subscriber's obligations

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

1. Correct and complete information: The Subscriber is responsible for delivering the requested information correctly along with the certificate signing request.

2. Certificate usage: The Subscriber is obligated to adhere to the restrictions set in section 5.3 in Certificate usage.

3. Diligence: The Certificate Subject is obligated to handle their Private Key diligently.

4. Key generation: The Certificate Subject 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.

5. Key length: The Certificate Subject is obligated to select 2048 bits as their keypair's length.

6. Key access control: The Subscriber is obligated to ensure that no one besides the Certificate Subject has a possibility to use the Certificate's Private Key.

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

    i. The Certificate Subject's Private Key is destroyed, goes missing, is stolen or its integrity is compromised in some other way or the key is othewise invalidated.

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

    iii. Certificate issuance prerequisites have changed.

8. The Subscriber is obligated to state their WS-channel username and/or Certificate serial number when making a Certificate revocation request. Informing of these details is a requirement for Certificate revocation.

6.3 Registration Authority obligations

Obligations for an RA that issues Certificates in adherence with the CP are:

1. To verify the Subscriber's identity and authorization to act on behalf of the organization they represent.

2. Making and archiving the Subscriber Agreement between the Subscriber and the bank.

3. Delivering the transfer keys required in Certificate application to the Subscriber.

4. Delivering the required documentation to Subscriber.

In addition, the system receiving the technical certificate signing request must confirm that the Subscriber's certificate signing request's signature has been created using the Certificate Subject's Private Key and that the transfer key matches the transfer key delivered by the registrar.

6.4 Relying Party obligations

By relying on the Certificate, the Relying Party expresses its acceptance of the terms of this CP.

The Relying Party is obligated to confirm throughout the entire Certificate chain, before accepting a Certificate:

1. Certificates' validity

2. Possible revocations or suspensions from Validation Authority and confirm the validity and integrity of the revocation information.

3. The Certificate's use case corresponds to the Certificate usage purposes stated in the Certificate.

4. The Certificate's usage purpose corresponds to the usage purposes defined in this CP (see section 5.3). 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.

5. Adherence to all precautions mentioned in the agreements or other Certificate-related documents.

6.5 CA's responsibilities

1. The CA is responsible for adhering to the procedures and practices described by the Root CA and this CP in its Certificate Services, unless not adhering to them is due to force majeure.

2. The CA is responsible for all actions performed using its Private Key.

3. The CA is responsible for identifying the Subscribers of the Certificates it has issued and confirming their authorization. The tasks in question are performed by RAs authorized by the CA.

4. The CA is responsible for ensuring that certificate services offered by it (see section 4.2) adhere to this CP.

5. The CA is in no way responsible for damages caused by the use of Certificates issued by it, unless the damages are caused by the CA acting in violation of this CP.

6. The 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.

6.6 Subscriber's responsibilities

1. The Subscriber is responsible for the usage and protection of the their Private Key for the duration of the Certificate's validity period.

2. However, the Subscriber's responsibility for the usage of their Private Key ends, when the CA has received a revocation request concerning the Certificate.

6.7 Relying Party responsibilities

By relying on the Certificate, the Relying Party expresses its acceptance of the terms of this CP.

1. It is the Relying party's responsibility to check the Certificate Chain.

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

6.8 Registration Authority responsibilities

1. The RA is responsible for ensuring that the Certificate Subscriber's and Certificate Subject's identities have been authenticated with due diligence and that the Subscriber's representative has the authorization to act on behalf of the End-Entity.

2. The RA is responsible for the registration event information storage and archival.

7 REQUIREMENTS ON CA PRACTICE

When issuing Certificates in adherence with this Certificate Policy, the procedures presented in this section are adhered to:

7.1 Certification practice statement

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 approves the CP and CPS.

4. CA reviews the CPS regularly and decides on required actions, such as performing of audits.

5. Certification practice statement is not a public document.

7.2 PKI key management life cycle

7.2.1 Generation and management of CA keys

Control objective: Certificate creation and management – the 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. The CA's keys are generated in a physically secure space (see section 7.4.4). Key generation is handled by persons appointed to the task (see section 7.4.3) under Dual Control. More detailed practices have been described in CPS.

2. The CA's keys are generated in an HSM device validated to at least FIPS 140-2 level 3 and configured to meet level 3 requirements.

3. 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 recommendations. More detailed descriptions can be found in the CPS.

4. 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). In addition, all key operation tasks are always performed under Dual Control, with the exception of Certificate and CRL signing as an internal function of the Certificate System and the activation of the CA's Private Key. Functions related to the CA's Private Key or its device environment are always recorded in a log.

5. 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.

6. 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. The CA's Private Key is protected using an HSM device dedicated only for the use of OP Services Ltd's CA Service.

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.

The CA Certificate is available to the End-Entities through the WS-channel. The CA Certificate and the Root CA Certificate are published at address: https://www.op.fi/varmennepalvelu.

7.2.4 Key escrow

Key Escrow is not in use for CA's or Certificate Subjects' Private Keys.

7.2.5 CA key usage

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

1. The CA's Private Key is used only for signing WS-channel's End-Entities' Certificates and CRLs containing said Certificates and for issuing OCSP Certificates.

2. The CA's private keys are only used in physically secure premises and in an HSM device.

3. The CA's key's activation data are under the control of a person in a trusted role.

7.2.6 End of CA keys' life cycle

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

All copies of 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: the 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 7.2.1, subsection 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 and initialization.

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: The Certificate Subject's Private Key is under their exclusive control.

1. The CA never stores the Private Keys of Certificate Subjects. (See section 7.2.4).

2. The Certificate Subject themselves generates the Certificate's Key Pair.

7.2.9 Certificate Subject's Private Keys' life cycle management

The Certificate Subjects' Private Keys are not handled in the CA's operations.

7.3 PKI Certificate life cycle management

7.3.1 Subscriber registration

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

1. The RA ensures that the Subscriber's representative's identity has been authenticated with due diligence and that the Subscriber's representative has the authorization to act on behalf of the Subscriber. In connection with the registration the RA records the Subscriber's and the Subscriber's representative's information and documents' authentication information in adherence with OP Financial Group's instructions.

2. The Subscriber accepts the Subscriber Agreement and possible other related service agreements.

3. The RA archives the agreement signed with the Subscriber.

4. The RA gives the Subscriber's representative the first part of the one-time shared secret needed in the Certificate's technical registration.

5. The RA Service's system sends the shared secret's second part to the mail address or SMS number stated by the Subscriber's representative or sends it by using secure email.

6. The Subscriber sends the technical certificate signing request to the WS-channel's RA Service's system that authenticates the identity of the Subscriber based on the shared secret.

7. The RA's system requests for a Certificate from the CA and delivers the issued Certificate to the Subscriber.

8. The CA stores the registration information for ten years after the registration event.

7.3.2 Certificate renewal, rekey and update

Creating a new Certificate always requires the generation of a new Key Pair. Certificate Modification without generating a new Key Pair is not possible either.

A Certificate can be renewed without renewing the Subscriber Agreement and identification in person as long as the old Certificate remains valid. In this case, the new certificate signing request is signed using the valid Private Key. The Subscriber's identity can also be authenticated using another CA-approved trustworthy method. In any other case, the Subscriber's identity must always be authenticated in person before Certificate issuance.

7.3.3 Certificate creation

Control objective: The CA ensures that the Certificates' issuing process is secure so that the integrity of the Certificates is retained. The issuance process comprises the following verifications:

1. Only unique serial numbers are used in Certificates issued by this CA and an unambiguous and unique information is associated with the Certificate Subject.

2. The CA ensures that the information content of the Certificates corresponds to the information received in connection with the registration.

3. In connection with the certificate signing request the Subscriber proves, using a CA-approved method, that it has under its control the Private Key that corresponds to the Public Key associated with the certificate signing request.

4. The Certificate System takes care of the Certificates uniformity in adherence with their usage purpose at a particular time.

5. Issued Certificates are valid at most for two years.

6. The Certificate Issuance process can be started only by authorized RAs whose identities are authenticated prior to Certificate creation.

7. The information content of the Certificates issued by the CA has been described in the CPS.

8. The integrity of the registration information is protected when the information is being delivered to the Certificate Subscriber/Subject or transferred between the CA's information systems.

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.

1. This CP and the Root CA's CP are available to the Subscriber at address: https://www.op.fi/varmennepalvelu

2. The Subscriber's responsibilities and obligations have been defined in the Subscriber Agreement in adherence to this CP.

7.3.5 Certificate dissemination

The CA does not publish the Certificate Subjects' Certificates.

The Certificates are delivered to the Subscribers through the WS Channel.

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. A Certificate revocation request can be made by a Certificate Subject, Certificate Subscriber, Certificate Subscriber's representative or the CA.
2. Certificate revocation requests can be made at a bank branch in person or over telephone or by calling the Revocation Service.
3. The maker of a revocation request must, when making the revocation request, state their name, the company they represent and their telephone number as well as the serial number of the Certificate they want revoked or their Web Services channel username. The revocation request is considered received only if all this information has been stated.
4. Revocation information is available to all Relying Parties through the VA.
5. The Revocation Service handles revocation requests without delay.
6. Revocation Requests are authenticated according to the CPS.
7. The CA can also offer a possibility to temporarily revoke (suspend) Certificates. The CA describes procedures related to this in the CPS.
8. 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. The CRL's validity time is three days and it is published at least once a day and upon each Certificate revocation.
   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.
4. The CA does its best to keep interruptions in the VA's services within the boundaries described in the CPS.
5. 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: The CA confirms that applied administrative and management practices are adequate and standards-compliant.

1. The CA performs risk assessments on its activities and defines the needed security requirements and practices.
2. The CA is responsible for its possible subcontractors' activities as for its own.
3. The CA operates according to predetermined practices in order to ensure quality and information security in production of the certificate service.

4. The 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: The CA ensures that its datasets and information are properly classified.

The 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. The 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 Financial 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. The CA's trusted roles are described unambiguously.

5. The 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 creation, Certificate Revocation management

Registration, acting as revocation service operator, certificate system administration tasks and the CA's governance tasks are the CA's trusted tasks.

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

2. The roles whose holders perform trusted tasks are defined in more detail in the CPS.

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

4. The persons acting in the CA's trusted tasks are trained for their tasks and have familiarized themselves with personnel security procedures in tasks that include security responsibilities. In addition, they have sufficient experience in information security and risk assessment.

7.4.4 Physical and environmental security

Control objective: The 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. The CA defines controls with which accidents, damages, risk to property and theft of or danger to data or production facilities are sought to be prevented.
2. Access to the CA's equipment is prevented from unauthorized persons.
3. Dual Control is adhered to in all operations related to the CA's HSM equipment, with the exception of the activation of the CA's Private Key.
4. When the HSM device is in storage, the storage space access control is under Dual Control.
5. All operations associated with CA equipment are documented.

7.4.4.2 Certificate production and revocation event management

1. Premises where Certificate creation or revocation management-related tasks are performed or where the CA's equipment is located have been physically secured, with access control, among other things, 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. 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.
4. 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

All workstations, servers and other system components connected to the certificate system that affect functions using which Certificates in adherence with this CP are issued, published and placed on the CRL are subject to the following principles while the environment is operational.

1. The CA secures the certificate systems' integrity and data against malware and unauthorized software.
2. The CA protects the telecommunications network connected to the Certificate System from unauthorized access, malware, attacks and unauthorized changes.
3. The CA monitors the systems' logs to detect anomalies.
4. The CA minimizes damages caused by information security breaches and malfunctions by using incident notification practices and action plans.
5. The CA monitors the system continuously to ensure its capacity and reliability.
6. CA protects the storage devices it uses from damage, theft and unauthorized use.
7. CA uses storage device management practices that prevent storage device lifepan running out or deterioration during document storage.

8. 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 section 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. The 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 tasks. CA ensures that access to system data and functions is restricted according to access management policy.

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

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

7.4.6.2 Certificate creation

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

7.4.6.3 Revocation information

Revocation information modification rights have been restricted using access control. However, no separate access rights are required for revocation information requests.

7.4.7 Reliable systems' usage and administration

Control objective: The CA uses reliable systems and products that have been protected against modification.

7.4.7.1 General matters pertaining to reliable 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: The CA ensures that in catastrophe situations, such as in the event of the CA's private key being compromised, 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

The CA has a regularly updated and tested continuity plan.

7.4.8.2 Backup and restoration of CA systems

The 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

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

Upon CA key compromise, the following actions are taken:

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

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.

3. The CA delivers its own Certificate's revocation request to the Root CA.

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, the Root CA 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, the CA ensures that maintenance of records needed for possible future investigations by authorities or legal proceeding continues.

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

1. The CA notifies the following parties of the termination of its activities at least 60 days prior to termination date: all Certificate Subscribers and Relying Parties with whom the CA has agreements or other established connections. In addition, the Root CA is notified of the termination.

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

3. The CA performs all of the needed actions in order to transfer the responsibility of the registration information maintenance (see 7.3.1) 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. The CA destroys or removes from use its Private Key as defined in section 7.2.6.

5. The CA requests for its Certificate's revocation from the Root CA if the CA's operations are terminated prior to the CA Certificate's expiration.

7.4.10 Applicable legislation

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

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

7.4.11 Information retention

Control objective: The 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

The 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 log files related to Certificates at minimum for 10 years from the file creation.

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 the 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

The 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. The current CP and earlier-published CPs.

4. Audit trail of the CA's activities.

7.4.11.3 Certificate production

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

1. Events related to the generation of the CA's private key and its renewal, including the 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. Backup 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

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

7.4.11.5 Certificate creation

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

7.4.11.6 Revocation service management

The 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 Services Ltd.

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.

All changes that require a notification are published at address:https://www.op.fi/varmennepalvelu

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

7.5.2 Version management

The CA archives all published and approved Certificate Policies.

Version	Date	Changes
1.0	9.4.2013	First approved version that is going to be published.
1.1	5.12.2016	Implemented corrections based on the review of the Finnish language version.
2.0	6.3.2017	Updated in 2016. Approved to be published.

7.5.3 Contact details

24/7 revocation service's telephone number: 010 252 8470

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

Postal address: OP / Jukka Ikäheimonen, P.O. Box 909, 00101 Helsinki

Telephone 010 252 010 (Jukka Ikäheimonen)