Samlink Customer CA
Version 1.1
7.11.2022

SAMLINK CUSTOMER CA

Certificate principles

WS MATERIAL SERVICES FOR CERTIFICATES

OID: 1.2.246.558.10.09704098.11.6

EFFECTIVE FROM 30.11.2022

samlink
A Kyndryl Company

Contents

LIST OF VERSIONS

Verification policy version information

Version number	Date	Changes
1.0	18.09.2009	Approved in the PKI steering group
1.1	26.10.2022	1. HTTP added, FIPS-140-1 -> 3 updated, added TLS, Certificate added pivate key 2 Updated RFC 2527 -> 3647 2.2 OID updated 2.4 Updated Risk & Security Department, Security Manager and contact info. Configuration of the PKI control group. 3.1.7 ldap -> http change 5.4.9 url update 7.1.6 FIPS 140-2 level 2 standard changed to FIPS 140-3 8.1.2 Publication address of the revocation list ldap→ http 8.1.3 change LDAPS -> HTTP
1.1	7.11.2022	Version 1.1 approved by the PKI Steering Group

1 CONCEPTS AND ABBREVIATIONS

A pair of keys	Consists of a Public and Private encryption key, which are mathematically related to each other in such a way that they can be used to perform encryption operations.
CRL	Certificate Revocation List. Block list, invalidation list, revocation list. List of decommissioned Certificates.
FIPS	Federal Information Protection Standard. FIPS-140-2 and FIPS-140-3 are security requirements for encryption modules and algorithms.
Index	Data warehouse, where Revocation Lists are published. The directory is available on the public information network.
HSM device	Hardware Security Module. A special device for protecting encryption keys.
HTTP	Hypertext Transfer Protocol. The Hypertext Transfer Protocol is a protocol used by browsers and WWW servers for data transfer.
Public key	Encryption key intended for public information. Data encrypted with a public key can only be read using its corresponding Private key. The public key is also used to check the electronic signature.
Corporate body	Legal entities, i.e. legal persons, are entities under commercial law (such as limited companies and cooperatives), entities under civil law (such as associations and foundations) and public entities (such as the state, municipalities or parishes).
LDAP	Lightweight Directory Access Protocol. Standard interface intended for directory use.
A trusted party	The entity that trusts the activities of the certifier and the Certificates it creates, as well as the entity that utilizes them.
OID	Object Identifier. A globally unique identification number.
Server management	The organization responsible for the infrastructure of Samlink or Samlink's customer company.

Server application	An application that can be used to sign, encrypt and process payment materials using certificates.
PKI	Public Key Infrastructure. The set of technical and administrative solutions related to the activities of the certifier.
PUK	PIN Unblocking Key. The code used to open a locked smart card.
Registrant	The entity responsible for Registration. Typically, the Registrant is the Bank when acting as the holder of Web-Services connection agreements. The registrant can also be Samlink.
Registration	The process that includes identifying the Certificate holder, collecting the necessary information and submitting it for the Certificate Request. Several Registration Officers may be involved in the registration.
Registration officer	The person responsible for registration tasks, e.g. checking the correctness of certificate requests and handing over certificates to the certificate holder. Acting as a registration officer requires an agreement between the bank and the Certifier on handling the task in the bank and a separate Service Agreement authorization from the employee. The person in charge of registration can also be a person designated by the Certifier as a trusted administrator.
RFC	Request For Comments. A collection of standards that e.g. define requirements for the operation of the Certifier.
RSA	An asymmetric encryption algorithm based on the use of Key Pairs.
Holder of contracts	The bank with which the customer enters into a Bank connection agreement and a Web-Services connection agreement
Closed list	See CRL
Locking service	Web-Services-connection The entity receiving the closing requests for contracts and Certificates.

Action card	A secure medium for storing private keys. Private keys are only used with smart card. Use requires activation of the key with a PIN number. Issued Certificates are also stored on the activity card.
Certificate	Information formed from the name of the certificate holder and the Public key, which the Certifier has signed electronically. A certificate proves that a particular Public Key belongs to a particular holder.
Verification policy	Describes the operation of the Certifier in compliance with the Certificate Principles.
Certificate service	The systems, people and processes related to the production of certificates as a whole. The sub-functions of the certificate service are Registration, Certificate production, Card production, Directory service, Revocation service and Revocation list service. A private key, also known as a secret key, is a variable in cryptography that is used with an algorithm to encrypt and decrypt data.
Certificate principles	Describes the requirements for issuing, producing and using certificates.
Certificate request	A request for the production of a Certificate sent by the Card Production or the Registrant to the Certificate Production, containing the information of the Certificate applicant and the Public key.
Certificate production	Certification production manages the certification system, produces Certificates and maintains their status information.
Certifier	The organization responsible for the certificate service.
Certificate applicant	A person for whom a Certificate is applied for, or a person who is authorized to apply for a Certificate for an element of the information network.
Certificate holder	The holder of the Private key corresponding to the Public key given in the Certificate, named in the Certificate.
Party relying on the certificate	The party relying on the certificate refers to a party that relies on the Certificates in accordance with the Certificate Principles in its transactions

Web-Services Connection Agreement	The agreement between the certificate holder (customer) and the Agreement holder (Bank), which is a prerequisite for ordering a WS-Data services certificate.
Private key	A key intended only for the holder's possession and use. The private key can be used to read the information intended for the holder, encrypted with the corresponding Public key. The private key can also be used to create the holder's electronic signature.
X.509	A standard that describes the requirements and components of the Certificate Service.
TLS	Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network.

In this document, the above concepts are written with a capital letter.

2 INTRODUCTION

These Samlink Customer CA Certificate Principles (hereafter Certificate Principles) are those of Oy Samlink Ab (hereafter. Samlink) regulations for issuing **WS-Data services** certificates and using these Certificates.

The certificate principles mainly cover the substantive issues related to the reliability and production of the certificate recommended by the standard RFC 3647 of the Internet Engineering Task Force.

2.1 GENERAL DESCRIPTION

Certificate principles are applied to WS-Data services certificates.

Samlink acts as a Certifier of Certificates according to the Certificate Principles. The certifier can use subcontractors in its operations.

The certification authority must prepare a description of its certification practices that comply with the certification principles.

2.2 IDENTIFIERS

The identifier of this document is *Samlink Customer CA Certificate principles WS-Data services for certificates, (OID 1.2.246.558.10.09704098.11.6, v.1.1)*

New versions of the certificate principles can be published. The effective date of the version in question is indicated on the cover page of the certificate principles. This and all previous published versions of the document can be read from the intranet pages used by Samlink and the banks, as well as through the distribution described in the Web-Services connection agreement.

2.2.1 The connection between the certificate and the corresponding Certificate Principles

The holder of the Certificate can verify that the Certificate complies with these Certificate Principles by checking that the content of the Certificate is in accordance with the certificate profile defined in chapter 8. " Certificate and blacklist profiles " in this document and that the Certificate was created during the validity period of these Certificate Principles.

When the new version of the certificate principles enters into force, all Certificates will be issued in accordance with the new version from then on. The moment the Certificate is issued is shown in the Certificate's validity period, and the version of the Certificate Principles valid at the time of issuance applies to that Certificate.

2.3 CERTIFICATION ORGANIZATION AND APPLICABILITY OF CERTIFICATES

2.3.1 Certifier

Samlink acts as a Certifier, which has overall responsibility for the delivery of the Certificate Service.

The Certifier can also issue Certificates other than those in accordance with these Certificate Principles. Separate Certificate Principles are drawn up for these Certificates.

2.3.2 Certificate production

Certificate production is a function that manages the technical system, produces Certificates and maintains their status information.

2.3.3 Registrant

Registrars may be Trusted for Registration activities within the Certifier's own organization and other entities authorized by the Certifier. If the certifier authorizes another party to act as Registrar, a separate agreement will be made for this.

Registrants undertake to comply with the Registrant's obligations mentioned in these Certificate Principles.

2.3.4 Certificate holder

The holder of Certificates in accordance with the Certificate Principles can be a legal entity that produces, mediates or processes payment materials or certificate system management transactions.

The certificate holder must comply with these Certification Principles of the Certification Authority and the Certification Policy of the Certification Authority.

2.3.5 A trusted party

A legal entity that produces, mediates or processes payment materials or certificate system management transactions can act as a trusted party that uses Certificates issued in accordance with the Certificate Principles.

The relying party must undertake to comply with its obligations described in this document.

2.3.6 Locking service

The CA's lockout service is a function that performs certificate revocation either using an automated process or by performing the revocation manually using a separate user interface made for this purpose. The revocation service must comply with the Certification Authority's Certification Principles and Certification Policy.

The contract closing service is a function that closes the Web-Services connection contract using an application made for this purpose. Closing the contract does not close the certificate, but closing the contract prevents the processing of all data signed with certificates related to the contract in the bank's information systems. The operator of the agreement's closing service is an entity authorized by the Certifier, which must comply with the Certifier's Certificate Principles and Certification Practice.

2.3.7 Index

The certificate service includes a directory in which the certificate blacklist is published and can be accessed from the public network.

2.3.8 Suitability

Certificates in accordance with the certificate principles can only be used in the Web-Services processing process of payment materials managed by Samlink, where the Certificates are used:

- Verification of the origin and integrity of information in electronic form,
- For encryption of information or keys in electronic form,
- Ensuring the confidentiality of information in electronic form.

When using certificates, you must take into account the certificate's "Key Usage" purpose of the key mentioned in the additional field.

Information that is encrypted with the key associated with the Certificate issued by the Certifier is not intended to be archived or stored in an encrypted form for a long time. The encryption cannot be decrypted if the decryption key is no longer available.

The Web-Services connection agreement may have restrictions related to the uses of the keys, which must be taken into account when using Certificates.

2.4 CONTACT INFORMATION

Samlink's Risk & Security Department is responsible for managing, maintaining and updating the Certificate Principles. The copyright of the certificate principles belongs to Samlink.

The certificate principles are approved by the Samlink PKI steering group appointed by the Samlink’s management team. PKI steering group consist of Samlink’s Head of Security and Head of Infra Management. Samlink's Security Manager acts as the presenter.

Questions about certificate principles can be sent to:

Oy Samlink Ab turvallisuus@samlink.fi
Box 130, Linnoitustie 9 Tel. (09) 548 050
02601 ESPOO Fax. (09) 5480 5853

Samlink's other contact information and service hours can be found at https://samlink.fi/en/contact-information/.

3 GENERAL CONDITIONS

3.1 RESPONSIBILITIES

3.1.1 Obligations of the certifier

The task of the Certification Authority issuing Certificates in accordance with the Certificate Principles is to:

- Providing Certificate and Directory services in accordance with the certificate principles
- Issuance and administration of Certificates in accordance with the Certificate Principles
- Cancellation of certificates and publication of Certificate Revocation Lists in accordance with these Certificate Principles
- ensures that the Certifier's Private keys are used only for signing Certificates and Exclusion Lists in accordance with the Certifier's Certificate Principles
- decide and carry out possible cross-certification with other Certifiers

The certifier is responsible for ensuring that the issued Certificates have been created in accordance with the requirements set out in the Certificate Principles and the information in the Web-Services connection agreement. The certifier is only responsible for the information recorded in the Certificate.

The Certifier is responsible for ensuring that when using the Key Pairs related to the Certificates appropriately, the Certificates will work from the moment of issue for the duration of the Certificate's validity, unless the Certificate is placed on the Revocation List.

The Certifier is responsible for ensuring that the Certificates requested to be revoked are taken to the Revocation List, which is published within the time specified in the Certificate Principles.

The Certifier is not responsible for damages resulting from the disclosure of the Private key, unless the disclosure is directly caused by the Certifier's actions.

The certifier is not responsible for indirect or consequential damages caused to the holder of the certificate. The Certifier is also not responsible for indirect or consequential damages suffered by the Party Relying on the Certificate, nor for damages that may be suffered by the other contractual partner of the Certificate holder.

The certifier is not responsible for the fact that the Certificate is used contrary to its intended use.

3.1.2 Obligations related to certificate production

The Certifier's obligations related to Certificate production are:

- Creation of a certification system corresponding to the certification principles, management and termination of operations in accordance with the Certification Principles
- Technical management of Certificates in accordance with the Certificate Principles throughout their entire life cycle (creation, storage, backup, publication and decommissioning)
- Technical production, maintenance and storage of the Revocation List in accordance with the certificate principles in the Directory
- maintaining a logbook of all management activities.

3.1.3 Responsibilities of the registrant

The responsibility of the Registrant participating in the issuance of Certificates in accordance with the Certificate Principles is:

- to be responsible for actions related to their own area of responsibility in accordance with the Certification Principles
- to take care of the correctness of the information in the Certificates.

The responsibilities of the registrants are summarized as follows:

- Verification of the certificate holder's identity and the person's right to act as the company's representative in this measure, in compliance with current legislation and the regulations of the authorities and instructions drawn up by their own organization
- making / checking the contract that is a prerequisite for registration
- secure delivery of registration information to the Certificate holder
- archiving of contract information related to registration

3.1.4 Obligations of the certificate holder

A person authorized by the organization in question is responsible for the responsibilities of the certificate holder, who must commit to the obligations below.

- Ensures that the information relevant to the identification of the certificate, which the holder of the certificate provides to the Registrant, is correct.
- Private and public key generation.
- Safe storage of the private key.
- Taking care of the safe storage of backups containing the private key.
- During its service period, the revocation service must make a notification to be delivered to the Certifier, if during the validity period of the Certificate:
  - there is reason to suspect that the Private key may have been exposed or used without permission,
  - The private key is corrupted or otherwise unavailable,
  - the authenticated device or server application is disabled.

- After the possible disclosure of the private key, its use is immediately and permanently terminated.

3.1.5 Obligations of the party relying on the certificate

It is up to the party relying on the certificate to trust the Certificates according to the Certificate Principles. In addition to what has been said elsewhere in the Certificate Principles, the following can be stated:

- The certifier complies with valid legislation in certification activities
- The certifier complies with the Certificate Principles
- The general security level of the certifier is remarkably high.

The person relying on the certificate is obliged to check the correctness of the Certifier and to check that the Certificate is valid, that the Certificate is not on the Revocation List and that the validity period of the Revocation List has not expired and that the key is used in accordance with its intended use.

When using Certificates in connection with Samlink's data network and services, Samlink can perform the aforementioned checks on behalf of the Relying Party.

3.1.6 Responsibilities of the locksmith service

The responsibility of the Closing service involved in closing Web-Services connection agreements in accordance with the certificate principles is:

- Performs the closing of the Agreement based on the mandate of the Certificate holder, the Certifier or the Registrar
- Ensures the origin and legality of the assignment
- Record completed assignments

3.1.7 Responsibilities related to the data warehouse

The certifier publishes the revocation lists in the Directory in accordance with section 2.3.7 " Directory ".

The directory can be accessed from anywhere using the HTTP protocol. The certification authority publishes the documentation regarding the Certificate Service through the distribution channels mentioned in section 3.6 " Publication of information and information storage ".

3.2 RESPONSIBILITY

3.2.1 Responsibility of the certifier

3.2.1.1 Checking the information contained in the certificate

By signing the Certificate with his Private Key, the Certifier shows that he takes responsibility for the correctness of the information in the Certificate in accordance with the Certificate Principles.

3.2.1.2 Liability limitations

The certifier is not responsible for damages resulting from actions contrary to the Certificate principles, terms of use or instructions.

The certifier is not responsible for indirect damages or damages that are the result of disruptions or errors in the certification operation caused by force majeure.

Other limitations of liability can be defined in a separate agreement, such as, for example, in the agreements of the Agreements closing service and the Agreements registration service.

3.2.2 Responsibilities of the registrant

The certifier is responsible for the operation of the registration points belonging to his own organization.

The organization of each registration point is responsible for the operation of the registration points managed by the certifier (banks).

3.3 FINANCIAL RESPONSIBILITY

The Certifier is not responsible for the financial commitments that arise when using the Certificate.

3.3.1 Damages

The certifier does not pay damages.

3.3.2 Reimbursements from the Certificate holder

If claims are made against the Certifier based on the points mentioned below, the Certificate holder undertakes to compensate the Certifier for all damages and costs arising from such claims and/or responding to them, including legal and legal fees.

- As a Trusted Party, the Certificate Holder has not checked the validity of the Certificate in accordance with the requirements of section 3.1.5 "Obligations of the Party Relying on the Certificate ".
- The certificate has been used contrary to the suitability defined for it or the intended use of the Public Key it contains.

– As a reliable party, the holder of the Certificate has relied on the Certificate otherwise without grounds given the circumstances.

The certifier informs the customer of the requirements in accordance with this paragraph in writing within a reasonable time after receiving information about them.

3.3.3 Relations between the parties

The functional, legal and financial relations between the Certifier, the Registrant, the Locking Service and the holder of the Certificate as well as the Certifier and possible subcontractors are defined in their mutual agreements.

3.3.4 Administrative processes

The certifier has defined and described the processes used in the verification activities and produced instructions corresponding to them.

3.4 INTERPRETATION AND ENFORCEMENT

3.4.1 Applicable legislation

Finnish law applies to these Certificate Principles.

3.4.2 Resolving disagreements

The resolution of disputes regarding these Certificate Principles is agreed upon in the agreements between the Certifier and the Certificate holder.

3.5 DUES

The certifier does not charge the use of the Certificate service directly from the holder of the Certificate, but the charges of the Certificate service are allocated to the holder of the Web-Services connection agreement in accordance with the currently valid price list.

3.6 DATA PUBLICATION AND DATA STORAGE

3.6.1 Publication of certifier's information

The certifier publishes the valid Certificate Principles on the intranet sites used by Samlink and the banks, as well as as stated in the Web-Services connection agreement. The previously valid Certificate Principles are also available from these addresses at least until the end of the life cycle of each Certificate issued according to the Certificate Principles.

Other possible descriptions and instructions related to the Certificate Service can also be published on the intranet websites used by Samlink and the banks.

The certifier publishes the Blacklist at the addresses indicated in section 5.4.6 "Blacklist inspection requirements" of the Samlink Customer CA Certification Policy document.

3.6.2 Publication frequency

Certificates published in the directory are published immediately after issuance. The blacklist is published in accordance with paragraph 5.4.8 " Publication of the blacklist".

3.6.3 Access control

Access control of the documents of the certificate service has been implemented so that the documents are only available to those who need to access them.

3.7 INSPECTIONS

Samlink's internal audit takes care of checking the activities of the certifier. With the help of the inspection, it is determined whether the certification organization operates in accordance with the Certification Principles.

The Certifier can inspect the activities of its Certificate holders and subcontractors with regard to activities related to the Certifier.

The entity responsible for the function is responsible for correcting the deficiencies that may have been detected during the inspection.

3.8 CONFIDENCE

In the processing of personal or identification data that may be processed in connection with the issuance or use of certificates, valid legislation is followed.

Information is disclosed to the authorities only based on laws, regulations and official regulations.

3.9 PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS

The ownership and intellectual property rights to the software, specifications and documents related to the certificate services belong to the Certifier or its suppliers or subcontractors in accordance with the agreements drawn up with them.

3.10 CONTRACTS

The holder of the Web-Services connection agreement makes a terms of use agreement with the holder of the Certificate, which describes the responsibilities and obligations of the parties. By signing the terms of use agreement, the Certificate holder accepts the conditions in the agreement and undertakes to act in accordance with them and these Certificate Principles.

The certifier draws up an agreement with potential subcontractors, which describes the responsibilities and obligations of the parties.

4 IDENTIFICATION AND AUTHENTICATION

4.1 NAMING POLICY IN THE CERTIFICATION AUTHORITY'S CERTIFICATE

The name of the Certifier issuing Certificates in accordance with the Certificate Principles can be found in both the "Issuer" and "Subject" fields of the Certifier's Certificate, as well as in the "Issuer" field of all other Certificates issued by the Certifier. The name consists of at least the following parts:

- Certification name (Common Name, CN),
- Certifier's organization (Organization Name, O)
- country (Country Name, C).

The exact contents of the parts are described below.

4.1.1 Certifier's Certificate identification information

Information (Attribute)	**Definition**	**Example**
Publisher (Issuer)	Certificate issuer	C=FI, O=Samlink, CN=Samlink Customer CA
Identifier (Subject)	The unique name of the certificate	C=FI, O=Samlink, CN=Samlink Customer CA
Serial Number (SerialNumber)	Unique identifier of the certificate	80:8e:c2:f0:14:25:e2:a3: 99:01:a5:12:06:71:19:39

4.2 FIRST REGISTRATION

4.2.1 Naming practices

In the Certificates issued according to the certificate principles, the unambiguous name in the "Subject" field contains the following information:

Information (Attribute)	**Definition**	**Example**
SurName (SurName)	The username recognized by the bank's Service Agreement System	SN=12345678
Common Name	Alphabetical name known by the bank's Service Agreement system	CN=Oy Firma AB
Organization	The plain name of the organization or organizational group	O=Pollution bank
Country	The country where the other organization operates	C=FI

The above-mentioned parts are mandatory in all Certificates issued in accordance with the Certificate Principles.

4.2.2 Name requirements

The identifier is the name registered in the Service Contract System, the correctness of which must be checked by the registrant when concluding the contract.

4.2.3 Unambiguity of names

In all Certificates issued by the Certifier, the user ID in the Surname field must be unambiguously linked to the contract, and the Service Agreement system ensures that the field is unambiguous. As an exception, Samlink's signature certificate for which there is no contract and the Surname field is given a value that will not appear in the Service Contract system.

4.2.4 Resolving name ambiguities

The certificate's identification information (user ID) is managed in the Service Agreement system, which ensures unanimity. If the name of the Certificate Request differs from the name of the Service Contract System, the Certificate will use the name known to the Service Contract System, if other information can be used to verify that the Certificate Request refers to the contract in question.

4.2.5 Proving possession of a private key

The certificate request is submitted to the Certifier signed with the Private key for which the Certificate is requested for the corresponding Public key.

4.2.6 Verification of the registrar

The identity of the registration officers is registered in Samlink's systems, and when logging into the registration officer's network, identification with their own identity is required.

The person in charge of registration must have a separate authorization to complete the registration in the Service Agreement system. The organization responsible for the registration point is responsible for managing the registrant's access rights.

4.2.7 Organization authentication

If the name of the certificate holder changes, the certificate holders can apply for new certificates by renewing the Web Services connection agreement related to the certificates. When the old agreement is terminated and a new Web-Services connection agreement is opened, new Certificates are issued and Certificates containing the old identification name are invalidated.

4.2.8 Identification of the certificate holder

The registrant identifies the Certificate holder's Web-Services connection at the time of signing the contract in compliance with the applicable legislation, regulations of the authorities and internal instructions given by their own organization.

4.3 RENEWAL OF THE CERTIFICATE UPON EXPIRATION

When the validity period of the Certificate is about to expire, the Certificate is renewed in such a way that the Key Pair is also renewed. Renewal of an expiring Certificate does not require renewal of the Service Agreement. The renewal request is signed with a valid private key,

4.4 RENEWAL OF THE CERTIFICATE AFTER ITS EXPIRATION OR CANCELLATION

Renewal of the Certificate after the expiry of the previous Certificate or cancellation of the Certificate takes place with the same procedure as for the first registration.

4.5 REQUEST TO SUSPEND THE VALIDITY OF THE WEB-SERVICES CONNECTION AGREEMENT

The contract closing service checks the validity of the Web-Services connection contract it receives, the origin of the suspension request, and the legality.
The request to suspend the validity of the Web-Services connection agreement is registered in the Agreement system. This registration immediately prevents the use of the service according to the Web-Services connection agreement with the Certificate related to that agreement after registration.
The holder of the certificate must notify the holder of the Web-Services connection contract about the suspension of the Web-Services connection contract.

If the request to suspend the Web-Services connection agreement is justified, the holder of the Service Agreement will terminate the Web-Services connection agreement, which will automatically result in a request to cancel the Certificate.

If the request to suspend the Web-Services connection agreement proves to be unjustified, the holder of the Web-Services connection agreement will set the Web-Services connection agreement to be valid, as a result of which the use of the certificates attached to the agreement will return to normal.

The terminated Web-Services connection agreement can no longer be restored, but a new agreement must be made, which starts the Certificate application process.

Termination of the Web-Services connection agreement does not cause any changes to the information in the Certificate or the Revocation List.

4.6 CERTIFICATE RESTORATION REQUEST

It is not possible to suspend the validity of the certificate, so the certificate cannot be returned to use.

5 FUNCTIONAL REQUIREMENTS

5.1 APPLYING FOR A CERTIFICATE

Applying for a certificate requires that the holder of the certificate, who has a valid Web-Services connection agreement, acts as the subscriber of the certificate.

5.2 ISSUING THE CERTIFICATE

The certification system only accepts such Certificate Requests, the origin of which can be identified from the electronic signature or the ID provided by the holder of the Web-Services connection agreement and the associated one-time password. The origin of the certificate request can also be identified using documents and personal identification.
The certificate can be issued in two different ways:

- Using the Web Services channel, where the certificate request and Certificate are forwarded with XML messages
- The Certificate holder submits the certificate request to the Certifier as e-mail attachments or on a separate data medium, and the Certifier submits the Certificate request to the Certificate holder as an e-mail attachment or on a separate data medium.

5.3 CERTIFICATE ACCEPTANCE

The Certificate holder is considered to have accepted the Certificate issued to him when:

- With the confirmation of the Bank Connection Agreement, the holder of the Certificate is committed to follow the instructions related to the use of the Certificate and
- The Certifier's information system has processed the Certificate request it received from the Certificate Holder and successfully returned the Certificate to the Certificate Holder and
- when the Certificate is installed for use, and
- The Private key corresponding to the certificate has been activated.

5.4 CANCELLATION OF THE CERTIFICATE AND SUSPENSION OF THE VALIDITY OF THE CERTIFICATE

The certificate can only be permanently revoked. Its validity cannot be suspended. Certificates that have been invalidated are published on the Revocation list in the Directory.

The certificate is always invalidated if the Web Services connection agreement related to the use of the certificate is terminated.

5.4.1 Circumstances for revoking the Certificate

The holder of the certificate must immediately request the cancellation of the certificate in the circumstances mentioned in the paragraph 3.1.4 "Responsibilities of the holder of the certificate" describing the notification responsibility related to the Revocation service.

5.4.2 The right to request the annulment of the Certificate

As a general rule, only a person who has the right to act as a representative of the Certificate holder can request the suspension or termination of the Web-Services connection agreement.

The cancellation request for the certificate and the closing request for the Web-Services connection agreement related to the certificate can be made by:

- Registrant under the terms of the Bank Connection Agreement
- Certificate holder
- The owner of the certificate service
- Samlink's Security Department.

If the cancellation request and the closing request of the Web-Services connection agreement related to the Certificate have been made by someone other than the Certificate holder, the Certificate holder will be notified.

5.4.3 Cancellation request procedure

The certifier must ensure that the Web-Services connection contracts are closed during the Locking Service's service time without delay based on the cancellation requests received.

As a rule, the cancellation of the certificate takes place as a result of the termination of the Web-Services connection agreement through a programmatic process, where the Certifier's information system acts as the sender of the certificate cancellation request. For exceptional situations, the Certifier's revocation service has an online tool that can be used to query individual certificate information and invalidate the certificate. The cancellation request must be submitted to the revocation service with a written notification containing the following information:

- subject of the request (username of the Web-Services connection agreement and holder of the Certificate)
- time of the request
- recipient of the request
- the person making the request and the method of identification
- the reason for the request.

5.4.4 Cancellation request waiting time

The contract closure service accepts cancellation requests during service hours. The contract closure service closes the Web-Services connection contract, which prevents the execution of processes using Certificates, but does not close the Certificate yet. After closing the Web-Services connection agreement, the termination of the Web-Services connection agreement must be notified to the holder of the Web-Services connection agreement, who terminates the Web-Services connection agreement. Upon termination of the Web-Services connection agreement, a certificate cancellation request is automatically generated.

The blacklist service takes care of the export of the certificate to the blacklist and the publication of the blacklist periodically in accordance with section 5.4.8 " Publication of the blacklist".

5.4.5 Circumstances for suspending the validity of the Certificate

It is not possible to suspend the validity of the certificate.

5.4.6 The right to suspend the validity of the Certificate

It is not possible to suspend the validity of the certificate.

5.4.7 Procedure for suspending the validity of the certificate

It is not possible to suspend the validity of the certificate.

5.4.8 Publication of the blacklist

The certifier offers a Closed List service, where information about closed Certificates is constantly available. Revocation lists are published regularly. The publication policy, publication frequency and validity periods of the blacklists are defined in section 5.4.8 of the Verification Policy. The integrity and correctness of the Revocation list information must be guaranteed.

5.4.9 Blacklist inspection requirements

A party relying on the certificate cannot rely on a Certificate whose validity has not been checked from the currently valid Revocation List.

Before trusting the Certificate, the Relying Party must ensure that the Certificate has not been placed on the Revocation List. The certificate cannot be trusted if the following blacklist information verification procedures are not followed carefully:

- A trusted party that searches the Blacklist from the Directory must verify the authenticity of the Blacklist by checking its electronic signature and the related verification path.
- The relying party must also check the validity period of the Blacklist to make sure that the Blacklist is still valid.
- Certificates can be stored locally in the Trusted Party's system, but before use, the current status of each such Certificate must be checked on the Revocation List in case of possible invalidation.

– If valid blacklist information is not available, e.g. due to a system or service failure, no Certificate should be trusted. Acceptance of the certificate contrary to this condition is at the Relying Party's own risk.

Revocation lists can be found at the following address:
URL= http://httpcrl.trust.telia.com/samlinkcustomerca.crl

Accepting the certificate without checking releases the Certifier from responsibility.

If a valid Revocation List is not available, the Certificate cannot be trusted.

5.5 RESTORING THE CERTIFICATE TO USE

It is not possible to suspend the validity of the certificate, so the certificate cannot be returned to use.

5.6 INFORMATION SECURITY CONTROL

Certificate production regularly stores and monitors relevant information generated in the certification operation and related to it. Some of this information is automatically saved in the production systems and some is saved manually by the staff of the Certification Production.

The stored data includes e.g. Information related to the life cycle of the Certifier's signing key, events related to the life cycle of all Certificates, and events related to data security maintenance.

In addition, Revocation service has the obligation to record the revocation requests of Web-Services connection agreements made by its own Revocation service managers.

5.7 DATA ARCHIVING

The Certifier (or Certificate Production on behalf of the Certifier) archives the most relevant information related to the certification activity.

The integrity of the information in the certificate archives is taken care of.

Events are archived in such a way that they cannot be deleted or destroyed during the period in which they are stored. Upon request, archives concerning certificates can be handed over to be used as proof of certification in court.

The archived information is kept protected against alteration and loss for the time required by legislation or authorities, however for at least three (3) years.

5.8 RENEWAL OF CA KEYS

The validity period of the Certifier's Certificate and the period of use of the Certifier's keys is a maximum of 25 years. A new Certifier's Key Pair and a Certifier's Certificate signed by the Certifier are created and published for at least the lifetime of the longest Certificate issued by the Certifier before the previous keys expire.

When changing the Certifier's Private key, care is taken to ensure that the verification chain is preserved between the old and new key.

5.9 DISASTER AND CA KEY EXPOSURE RECOVERY

The certifier is responsible for ensuring that in emergency situations, which include e.g. If the Certifier's Private Key is revealed or falls into the wrong hands and computer resources, software and/or data are destroyed, the operation of the Certificate Service will be restored to normal as quickly as possible.

5.9.1 Computer hardware, software, and/or data are corrupted

The certifier must take care of securing its most critical systems in terms of business continuity, backing up software and saving data so that their recovery from the backup is possible.

5.9.2 The private key of the certificate authority has been exposed

The Certifier must create operational instructions in case the Certifier's Private key is revealed, which include at least the following tasks:

- immediately inform the holders of the Certificate and other Certifiers, with whom the Certifier may have an agreement, of the disclosure,
- disabling the revocation list
- New keys and Certificate must be created for the certifier
- Certificates issued from the certificate system that are valid at the time in question must be renewed.

5.10 TERMINATION OF VERIFICATION ACTIVITIES

Termination of certification activities is considered a situation where all services related to the issuance of Certificates by the Certifier are permanently terminated. Termination of certification activities does not mean a situation where the Certification Service is transferred from one organization to another.

The Certifier shall notify the Certificate holders and all parties with whom the Certifier has agreements or other established relationships related to Certificate services in writing about the termination of the certification activities. Notification of the termination of the verification activity must be made to the aforementioned entities as soon as possible, however at least six (6) months before the date of termination.

The Certifier terminates all authorizations concerning activities outsourced by the Certifier in connection with the process of issuing Certificates.

The Certifier ensures that the Certificates it issues can no longer be used reliably.

Upon termination of the certificate service, Certificate Production destroys or deactivates the Private key of the Certifier.

The Certifier terminates the Web-Services connection agreements concluded with the holders of the Certificate in accordance with the notice period stated in the agreements.

6 SAFETY MEASURES

The following points apply to the Certifier and any subcontractor responsible for Certificate production.

6.1 PHYSICAL SECURITY SOLUTIONS

Physical access to critical services is monitored and physical risks to the Certificate production system are minimized. This requires e.g. ensuring the following protective measures:

- Physical access to the premises related to the creation of Certificates must be limited so that only authorized persons can access the premises.
- Sufficient protective measures must be implemented to prevent equipment or software belonging to the Certifier's and Certificator's systems from being broken, destroyed, or compromised, and business interruption that may result from them.
- Hardware, information, data media and software related to certificate services must be protected from unauthorized removal from the premises.
- Sufficient security measures must be in place to prevent the disclosure or theft of data and break-in to the premises used for data processing.
- In order to protect the resources offered by the production facility and the actual system resources, security monitoring related to the production environment must be organized.

Fulfilling the requirements described above requires measures, e.g. in the following areas, the implementation of which is described in more detail in the Certification Policy:

- The location and structure of the equipment compartment
- Physical access control
- Electricity supply and air conditioning
- Protection against water damage
- Fire safety
- Storage of information material
- Disposal of waste material
- Backups stored elsewhere

6.2 FUNCTIONAL SECURITY SOLUTIONS

6.2.1 Trusted managers

Listed administrators are all those who are responsible for ensuring, maintaining and supervising the operation of the Certificate Service.

The following Trusted Administrators, whose responsibilities are described in the Verification Policy, participate in the verification activity:

- Information security officer
- System administrator
- System manager
- System Evaluator
- Registration officer
- Revocation service manager

Trusted managers undertake to comply with the Certificate Principles.

6.2.2 The number of persons required for the tasks

To perform the following procedures, at least two people are required to be present at the same time:

- Changes to the Certifier's production system environment

- Backing up and restoring the Certificate Authority's Private Key

At least four people are required to be present at the same time to perform the following procedures:

- Creation of CA keys

6.2.3 Identification and authentication of trusted agents

Identification of the most important trusted action holders requires the use of a Certificate. Identification related to different activities is described in the Verification policy.

6.3 PERSONAL SAFETY

6.3.1 Background check procedure

The certifier and potential subcontractors perform the necessary checks for all the persons they hire in accordance with their personnel policies. The inspection examines the person's reliability and professionalism.

People in key trusted roles are subject to background checks. These roles are defined in the Certification Policy. Persons who do not pass the initial inspection or a possible inspection at a later stage cannot act or continue as trusted administrators.

6.3.2 Educational requirements

Personnel must be properly trained in the hardware and software environment related to the Certificate Service.

6.3.3 Consequences of unauthorized actions

If the Certifier or a possible subcontractor responsible for Certificate production discovers abuses related to the certification activities, they will immediately take the necessary measures to remove the harm caused by the abuses and to prevent their recurrence.

6.3.4 Contract worker requirements

The requirements of contract workers are the same as the requirements of permanent personnel.

7 TECHNICAL SECURITY SOLUTIONS

7.1 CREATION, IMPLEMENTATION AND PROTECTION OF THE CERTIFICATE AUTHORITY'S KEY PAIR

7.1.1 Creating a CA Key Pair

The Certifier must ensure that the Certifier's keys are created under controlled conditions.

In particular, it must be taken into account that the creation of the Certifier's keys takes place in a physically secure environment by trusted operators. Completing the task requires at least four people to be present at the same time. The number of trusted operators who are authorized to perform this action must be limited to the minimum possible.

7.1.2 Delivery of the Certifier's Public Key to Relying Parties

The Certifier ensures that the integrity and authenticity of the Certifier's Public Key and all related parameters are preserved when the key is made available to Relying Parties.

The Certifier's Certificate, which contains the Certifier's Public Key, is available to Relying Parties.

7.1.3 The lengths of the certifier's keys and the algorithm used

The length of the CA's signing key and the algorithm used with the key must be chosen in such a way that they are considered generally applicable to certificates.

7.1.4 Lifetime of the Certifier's Key Pair

Certificates can be signed with the Certifier's Private key for the lifetime of the Certifier's Key Pair minus the longest validity period of the Certificate holder's Certificate. After this, the Certifier must create a new Key Pair for signing the Certificates. Revocation lists are signed with a Private key throughout the lifetime of the Certifier's Key Pair. The lifetime of the Certifier's Private key and the validity period of the Certifier's Certificate are defined in the Certification Policy document.

7.1.5 Purposes of the certifier's keys

The Certifier ensures that the Certifier's signing keys are not used for purposes other than the issuance of Certificates and the publication of Revocation List information, and that the Certifier's signing keys are only used in physically secure premises.

7.1.6 Protecting the Certificate Authority's Private Key

The certificate production must ensure that the Certifier's private keys remain confidential and intact.

When the Private Signing Key is outside of a secure signature creation tool, it must be encrypted using an algorithm and key length known to withstand encryption attacks for the lifetime of the key or part of the key.

The Certifier's Private Signing Key can only be verified, stored and restored by trusted agents in a physically secure environment. Performing these procedures requires at least four people to be present at the same time. The number of trusted agents who are authorized to perform these procedures must be limited to the minimum possible.

At least the same level of security mechanisms are applied to the backups of the Certifier's Private Signing Key as to the signing keys in use.

When the keys are stored on the hardware intended for key processing, access control ensures that the keys cannot be accessed from outside the hardware.

The private signing key of the certificate authority must be protected by an HSM device (Hardware Security Module) that complies with at least the FIPS 140-3 standard.

7.1.7 Storage of the Certificate Authority's Private Key by a third party

The Certifier's private signing key is not given to third parties for safekeeping in such a way that it would be available to persons outside the Certifier's operations under certain circumstances (the method is called key escrow).

7.1.8 Backing up the private key of the CA

Backups of the CA's Private key are taken so that restoration from the backup can be done with the same level of security as the transfer of the CA's Private key.

7.1.9 Transfer of the Certificate Authority's Private Key.

The Certifier must ensure that the Certifier's keys are transferred under controlled conditions and that the keys are never in plain sight in one place. The keys must be either encrypted or divided into several separate parts that are transferred separately.

In particular, it must be taken into account that the transfer of the Certifier's keys takes place in a physically secure environment by trusted operators. Completing the task requires at least two people to be present at the same time. The number of trusted operators who are authorized to perform this action must be limited to a minimum

7.1.10 Archiving of the CA's Private Key

The private key of the certificate authority is not archived.

7.1.11 Activation of the private key of the certificate authority

The Certifier's Private key is activated at the same time as the keys are created according to section 7.1.1 " Creating the Certifier's Key Pair ". The key remains active until its use is interrupted, e.g. due to maintenance procedures.

7.1.12 Deactivation of the private key of the certificate authority

Deactivation of the Certifier's Private key is done if necessary, e.g. due to maintenance procedures.

7.1.13 Destruction of the Certificate Authority's Private Key

Certificate production ensures that the Certifier's Private Signing Keys are destroyed or that they are not used after the end of their life cycle.

7.1.14 Archiving of the Public Key of the CA

The Certifier archives valid and expired Certifier Public Keys in accordance with section 5.7 " Data Archiving ".

7.2 CREATION, ACTIVATION AND PROTECTION OF THE CERTIFICATE HOLDER'S KEY PAIR

7.2.1 Creating a Certificate Holder's Key Pair

The holder of the certificate is responsible for the secure creation of the Key Pair and maintaining the confidentiality of the Private Key.

The certificate holder's private key is never delivered to the CA.

7.2.2 Delivery of the public key of the certificate holder to the Certifier

The holder of the certificate, who creates the Key Pair, delivers to the information system of the Certifier via the WS channel a Certificate Request containing the Public key, the origin of which is checked with an electronic signature or a one-time use ID and password, in an XML message. The certifier's information system sends the Certificate request containing the Public key of the Certificate holder with an XML message via an encrypted connection to the certification system.

7.2.3 The lengths of the certificate holder's keys and the algorithm used

The length of the certificate holder's Private Key and the algorithm used with the key must be chosen in such a way that they are generally considered sufficiently secure.

7.2.4 Lifetime of the certificate holder's Key Pair

The lifetime of the certificate holder's Public and Private keys is the same as the validity period of the related Certificate. Public and Private keys may no longer be used if the encryption algorithms and related parameters are no longer sufficiently strong or otherwise suitable.

7.2.5 Purposes of the certificate holder's keys

Private keys related to Certificates issued according to these Certificate Principles can only be used to implement the following security services:

– Verification of the origin and integrity of information in electronic form

- Ensuring the confidentiality of information in electronic form.

7.2.6 Protecting the private key of the certificate holder

- The holder of the certificate must protect the Private key associated with the certificate.

7.2.7 Backing up the private key of the certificate holder

The holder of the certificate is responsible for keeping his Private key.

7.2.8 Archiving of the certificate holder's Private Key

The Certificate holder's Private key is not archived by the Certification Authority.

7.2.9 Destruction of the private key of the certificate holder

The holder of the certificate is responsible for destroying his Private key.

7.2.10 Archiving of the certificate holder's Public Key

The Certifier archives the Certificate holder's Public Key in accordance with section 5.7 " Data Archiving ".

7.3 SECURITY SOLUTIONS FOR INFORMATION SYSTEMS

The certifier uses reliable systems and products that are protected against changes. In particular, the following aspects have been taken into account:

- identifying all users
- role-based access control
- the supervision of several people required by critical functions
- creating audit logs, viewing audit data and archiving security-related events
- backups, backup systems and recovery
- secure destruction of data when it is no longer needed.

7.4 LIFECYCLE MANAGEMENT SECURITY SOLUTIONS

7.4.1 System development management

Certificate production uses reliable systems and products that are protected against changes.

There are change management practices for new updates, versions and installable patches of all software related to operation.

7.4.2 Information security management

7.4.2.1 Information security maintenance

The Certifier and any subcontractor responsible for Certificate production must ensure that management and maintenance practices are adequate and secure.

7.4.2.2 Resource management

The certifier is responsible for ensuring that the protection level of resources and information is sufficient.

7.4.2.3 User service management

Certificate production is responsible for ensuring that its systems are secure and carefully maintained and that the risk of malfunction is minimal. Adequate operating models and practices are created and implemented for trusted task managers. The data integrity of the verification system is protected from viruses and unauthorized programs that damage the system. All storage devices, data media and data repositories are handled carefully to prevent damage, theft and unauthorized use.

Capacity usage is monitored and future capacity needs are assessed to ensure that sufficient processing power and storage capacity are available.

In certificate production, the operations related to information security must be separated from the normal operation operations of the systems.

7.4.2.4 System access control

The certifier and any subcontractor responsible for certificate production ensure that only certain authorized persons have access to the systems. User management of the systems includes the creation of user IDs, usage monitoring and timely change and deletion of user rights.

The systems must have sufficient security procedures to separate the roles of the administrators defined in section 6.2.1 " Trusted administrators". Especially in Certificate production, the role of the information security administrator must be kept separate from the operating functions. Personnel identification must be completed successfully before they can use critical programs related to Certificate Management.

The application used to issue the Certificates uses access control to prevent unauthorized attempts to remove, add or change the Certificates or related information.

The application used for the blacklist service uses access control to prevent unauthorized changes to the Blacklist data.

7.4.2.5 HSM device lifecycle management

Certificate production takes care of the data security of the HSM device used for signing Certificates and Revocation Lists throughout its life cycle in such a way that:

- The device cannot be accessed during its delivery or storage in such a way that it would not be detected.
- Installing, verifying and restoring the CA's signing keys to the device requires at least four people to be present at the same time.
- The device works correctly in use.
- The Certifier's private signing keys stored in the device are destroyed when the device is deactivated.

7.5 TELECOMMUNICATION NETWORK SECURITY SOLUTIONS

The certifier and any subcontractor responsible for certificate production take care of network security management, e.g. with the following measures:

- The internal network of certificate production is protected from external networks used by third parties.
- Confidential information is protected when it is transmitted over unsecured networks.
- Certificate production is responsible for keeping its local network components (e.g. routers) in a physically secure environment.
- In certificate production, systems are monitored for unexpected events that may occur in them with the help of continuous monitoring, supervision and alarm equipment. Such events include e.g. unauthorized access attempt or abnormal use of resources.

8 CERTIFICATE AND BLACKLIST PROFILES

All Certificates issued by Samlink Customer CA comply with the X.509 standard. The certificates meet the requirements of the document RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

The Revocation Lists published by Samlink Customer CA are always formed complete with the normal version 2 format of the PKIX standard, so that the hashing algorithm is SHA256.
The detailed profile of the revocation list is described in section 8.1.3.

8.1.1 CA certificate

One CA certificate is associated with the Samlink Customer CA system, which uses the following fields:

Field name	**Field name**	**The content of the field**
Version	Version	3
Serial number	Serial number	80:8e:c2:f0:14:25:e2:a3:99:01:a5:12:06:71:19:39
Signature algorithm	Signature algorithm	sha256WithRSAEncryption
Certificate issuer	Issuer	C=FI, O=Samlink, CN=Samlink Customer CA
Validity period	Validity	Not Before: Aug 18 08:00:35 2009 GMT Not After : Aug 18 08:00:35 2034 GMT
Certificate holder	Subject	C=FI, O=Samlink, CN=Samlink Customer CA
Certificate holder's Public Key information	Subject public key info	Public Key Algorithm: rsaEncryption RSA Public Key: (4096 bit)
Certificate Authority's Public Key Identifier	Authority key identifier	keyid:CA:80:38:33:93:8A:63:04:91:8D:05:69:56:68:42:35:E5:C7:FF:BC
Public key identifier of the certificate holder	Subject key Identifier	CA:80:38:33:93:8A:63:04:91:8D:05:69:56:68:42:35:E5:C7:FF:BC
Key purpose extension	Key usage	critical Digital Signature, Certificate Sign, CRL Sign

8.1.2 User certificate

Fields used in the WS-Data services certificate:

Field name	Field name	The content of the field
Issuer	Issuer	CN=Samlink Customer CA, O=Samlink, C=FI
Key length	Key	2048 bits/RSA
Gaskets	Signature algorithm	SHA256
A unique name	DN	SN,CN,O,C (values from the Bank's contract system); others upon request
Extensions		
Public key identifier of the certificate holder	Subject Key Identifier	Key hash in 20 bytes
Identifier of the CA's public key	Authority Key Identifier	KeyID=02 aa 0c 9e bd e9 48 81 27 08 28 e6 e8 de 14 f7 15 8c b9 b6
Publication address of the revocation list	CDP CRL distribution points	URL= http://httpcrl.trust.telia.com/samlinkcustomerca.crl
The purpose of the key	Key usage	Critical; Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment
CP – certificate policy identifier		As a value: Samlink Customer CA Certificate Principles WS-Data Services for certificates OID: 1.2.246.558.10.09704098.11.2 V.1.0

8.1.3 Revocation list profile

The CRL lists are published from the CA system to the public directory maintained by Certificate production, which is referenced in the CDP field of the certificates (see values from the certificate definition).

Publications are made using the HTTP protocol. The source address is http://httpcrl.trust.telia.com/samlinkcustomerca.crl .

The CRL lists are always created complete with the normal version 2 format of the PKIX standard, so that the hash algorithm is SHA256. The fields used are:

Field name	Field name	The content of the field
Version	Version	V2
Signature algorithm	Signature algorithm	SHA256

Revocation list publisher	Issuer	CN = Samlink Customer CA
		O = Samlink
		C = FI

Publication time of the closed list	Effective date	CRL creation time
Publication time of the next Closed List	Next update	CRL expiration date (5 days from creation)
Revoked Certificates	Revoked certificates	
Revocation list signing key identifier	Authority key identifier	ca 80 38 33 93 8a 63 04 91 8d 05 69 56 68 42 35 e5 c7 ff bc
Revocation list sequence number	CRL number	Running CRL sequence number

In accordance with the PKIX recommendation, serial numbers of expired certificates are automatically removed from CRL lists.

9 ADMINISTRATION OF CERTIFICATE PRINCIPLES

9.1 CHANGE PROCEDURE

The certifier can change the specifications due to legislative or operational requirements. Configuration changes must be recorded in the Certificate Principles and Certification Policy documents as described below.

If, in the opinion of the approvers, a minor change is made to the document, the revision number (decimal part) of the document is increased. If the change is greater, the version number (entire part) of the document is increased

A minor change can enter into force immediately after it has been approved and changed and the new Certificate Principles have been published. A major change is notified at least 15 days before it enters into force.

9.1.1 Items that can be changed without an approval procedure

Corrections related to spelling and layout, as well as changes to contact information can be made to this document without an approval procedure.

Translations of the document can be published in different languages without a separate approval procedure. If the translation and the Finnish text contradict each other, the Finnish text is valid.

Renewal of the certification practice does not require notification.

9.1.2 Changes that require a new Certificate Principles document to be drawn up

The new Certificate Principles document gets a new OID. The Certificate Principles are new if the previously issued certificates no longer fit within the scope of the new Certificate Principles.

Renewal of the certification policy does not require the preparation of a new Certification Principles document.

9.2 APPROVAL PROCEDURE

All changes to these Certificate Principles, with the exception of changes related to appearance, spelling or contact information, must be approved by the Samlink PKI steering group. Samlink's director of security acts as the presenter.

9.3 PUBLICATION

The certificate principles are published for the parties who are required to comply with them, on the intranet sites used by Samlink and the banks, on the public website or in another separately agreed manner. The previously valid Certificate Principles are also available from the aforementioned addresses at least until the end of the life cycle of each Certificate issued according to the Certificate Principles.

Other possible descriptions and instructions related to the Certificate Service can also be published on the intranet websites used by Samlink and the banks.

Upon separate agreement, the certificate principles can also be delivered via another data medium directly to the parties who are required to comply with it.