Samlink Customer CA
Version 1.1
7.11.2022

SAMLINK CUSTOMER CA

Verification policy

OID: 1.2.246.558.10.09704098.11.5

EFFECTIVE FROM 30.11.2022

samlink
A Kyndryl Company

Table of 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 and SSW changed to CM, FIPS-140-1 -> 3 updated, added TLS, Certificate added private 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. 5.4.6 url ldap→ http 6.1.1 Updated to TRAFICOM/54045/03.04.05.00/2020 etc. 7.1.6 FIPS 140-2 level 2 standard changed to FIPS 140-3 8.1.1 Revocation list Publication location ldap→ http 8.2 ldap → 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.
CA	Certificate Authority, Certifier - a trusted neutral third party that issues and maintains electronic certificates and other related services (registration, public key directories, revocation lists)
CRL	Certificate Revocation List. block list, invalidation list, revocation list. List of decommissioned Certificates.
FIPS	Federal Information Protection Standard. FIPS-140-1 and FIPS-140-3 are security requirements for encryption modules and algorithms.
Index	A data warehouse in which e.g. Certificates and revocation lists.
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.
Adoption	Samlink's PKI steering group approves the changes made to the document. The certifying agent is responsible for maintaining the document. Certificate production and the certifier take care of the necessary updates and deliver the updated document to the responsible person of the certifier. After approval, the person in charge of the certifier delivers the document to the person in charge of the architecture of the certificate production.
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).
Device	Device refers to a physical device, such as a workstation or server
LDAP	Lightweight Directory Access Protocol. Standard interface intended for directory use.

LDAPS	SSL protected (encrypted) version of the LDAP protocol
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	Server means a service whose instance can be run on several different devices
Server management	The organization responsible for the infrastructure of Samlink or Samlink's customer company.
Service agreement	Agreement for the service, the use of which requires the use of the certificates described in this document
PKI	Public Key Infrastructure. The set of technical and administrative solutions related to the activities of the certifier.
Registrant	The entity responsible for Registration.
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 collecting and registering information for the Certificate Request.
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.
Samlink's customer company	Samlink's customer company refers to companies to which Samlink supplies information systems or information system services.
The holder of the service contract	As a rule, the holder of the service contract is the bank, but Samlink can also act as the holder of the service contract.
Bank	The bank acts as a service provider using Certificates. The holder of the certificate acquires the certificates by signing a Service Agreement for the service whose use the certificates are related to
Contract closing service	The entity that receives service contract closure requests, which the certifier has authorized with a separate agreement.

Contract system	Information system used to register the Service Agreement for the Certificate holder for the service for which the certificates described in this document are used
Application	Application means a program whose different instances can be run on several different devices.
SSL	Secure Sockets Layer, an information security protocol commonly used on the Internet
CM	Telia Certificate Manager, the information security service for certificate production, with which most certificate management software for certificate production is protected.
Revocation list	See CRL
Revocation service	The entity receiving certificate revocation requests.
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. 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 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, Directory service, Revocation service and Revocation list service.
Certificate principles	Describes the requirements for issuing, producing and using certificates.
Certificate request	Information of the applicant for the certificate and the request containing the public key for the production of the certificate.
Certificate production	Certification production manages the certification system, produces Certificates and maintains their status information.
Verification policy	Describes the operation of the Certifier in compliance with the Certificate Principles.
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
X.509	A standard that describes the requirements and components of the Certificate Service.
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.
TLS	Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network.

2 INTRODUCTION

This Samlink Customer CA Certification Policy (hereinafter referred to as the Certification Policy) is a description approved by Oy Samlink Ab (hereinafter referred to as Samlink) of the practices that are followed when issuing and using Certificates in accordance with the Samlink Customer CA Certificate Principles (hereinafter referred to as the Certificate Principles).

The Certifier (Samlink) and its possible subcontractors, as well as the holders of the Certificate and parties relying on the Certificate, must comply with this Certification Policy in connection with the Certificates issued by the Certifier.

The structure of the certification policy follows the structure used in Samlink's Certificate Principles, which mainly covers issues related to the reliability and production of the Certificate recommended by the Internet Engineering Task Force standard RFC 3647.

The certificate service has taken into account the technical and administrative requirements required to produce the Quality Certificate.

2.1 GENERAL DESCRIPTION

This Certification Policy applies to Certificates issued by Samlink as a Certification Body in accordance with the Certification Principles it has prepared.

The certifier can use subcontractors to implement the Certificate Service.

2.2 IDENTIFIERS

The identifier of this document is *Samlink Customer CA Certification Policy*, whose unique identifier is OID 1.2.246.558.10.09704098.11.5 v.1.1

The certification policy is available to all parties who are required to comply with it.

2.3 CERTIFICATION ORGANIZATION AND APPLICABILITY OF CERTIFICATES

2.3.1 Certifier

The Certifier operating in accordance with this Certification policy is Samlink. In the Certificates issued by the Certifier, the name of the Certifier is " *CN = Samlink Customer CA, O = Samlink, C = FI* ".

In addition to issuing and publishing certificates, the Certifier also ensures that a Revocation service is available for Certificate holders and a revocation list service for Trusted parties.

2.3.2 Certificate production

Certificate production manages the Certificate production system, creates and publishes Certificates and maintains their status information throughout their life cycle. Certification production undertakes to comply with this Certification policy for its part.

2.3.3 Registrant

The registrar handles the identification of the Certificate holder, the collection of the necessary information and their delivery for the Certificate request. Several Registration Officers may be involved in the registration.

Registrants may be persons authorized for Registration activities belonging to the Certifier's own organization and other entities possibly authorized by the Certifier.

All Registrants are obliged to comply with this Verification Policy.

2.3.4 Certificate holder

Certificate holders are defined in the Certificate Principles. The Private key corresponding to the Public key contained in the Certificate is intended for the exclusive use of the Certificate holder.

2.3.5 A trusted party

Relying parties using Certificates issued by the Certifier are defined in the Certificate Principles. The relying party must undertake to comply with its obligations described in this document.

2.3.6 Revocation service

Those working in the revocation service are obliged to comply with this Verification policy for their part.

The revocation service is defined in more detail in the Certificate Principles.

2.3.7 Index

The certifier publishes the Certificate Closure Lists in the Directory.

2.3.8 Suitability

Certificates issued by the Certifier can only be used in the following functions:

- 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.

The applicability of different certificate types is described in the relevant Certificate Principles

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

A file or message that is encrypted with a key related to 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 agreement regarding the certificate service may have restrictions related to the uses of the keys, which must be taken into account when using the Certificates.

2.4 CONTACT INFORMATION

Samlink's Risk & Security Department is responsible for managing, maintaining and updating this Verification Policy. The copyright for this Verification Policy belongs to Samlink.

The verification policy is approved by the Samlink PKI steering group appointed by 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 regarding this Verification Policy 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 Certifier's obligations regarding the various Certificates are defined in the relevant Certificate Principles in section 3.1.1.

3.1.2 Obligations related to certificate production

The obligations related to certificate production are defined for each type of certificate in its own Certificate Principles in chapter 3.1.2.

3.1.3 Responsibilities of the registrant

The registrant's obligations are described in the Certificate Principles in paragraph 3.1.3

3.1.4 Obligations of the certificate holder

The certificate holder's responsibility is set in the Certificate Principles to the administrator of the system element in question. Compliance with this responsibility requires the following measures:

- The administrator must ensure that a backup copy of the Private key is available.

- The administrator must immediately make a Certificate revocation request to the Contracts revocation service during its service period, when the Private key has been corrupted or disabled, or there is reason to suspect that it has been compromised.

- The administrator must notify the service provider of the termination of the service. Termination of the service also automatically causes a request to revoke the certificate.

- The administrator must dispose of the Private key and Certificate from the device or server application after the Certificate expires or when the Certificate is no longer needed for the original purpose of use.

3.1.5 Responsibilities of the revocation service

The responsibilities of the revocation service are defined in the Certificate Principles in chapter 3.1.6.

3.1.6 Obligations of the party relying on the certificate

The obligations of the party relying on the certificate are defined in the Certificate principles in chapter 3.1.5.

3.1.7 Responsibilities related to the data warehouse

The obligations related to the data warehouse are defined in the Certificate Principles in chapter 3.1.7.

3.2 RESPONSIBILITY

The responsibilities of the Certifier and the Registrant are described in the Certificate Principles in chapter 3.2.

3.3 FINANCIAL RESPONSIBILITY

The financial responsibility is described in the Certificate Principles in chapter 3.3.

3.4 INTERPRETATION AND ENFORCEMENT

3.4.1 Applicable legislation

Finnish law applies to this Verification Policy.

3.4.2 Resolving disagreements

If disagreements arise between the Certificate holder and the Certifier regarding the Certificate Service, they will primarily be resolved through negotiations. If an agreement cannot be reached on disagreements, the agreements between the Certifier and the holder of the Certificate will be followed in their resolution.

3.5 DUES

Fees for certificate services are charged according to the service price list valid at any given time. The charging criteria are described in more detail in the Certificate Principles in chapter 3.5

3.6 DATA PUBLICATION AND DATA STORAGE

The publication of information is described in Certificate Principles in chapter 3.6.

3.7 INSPECTIONS

Samlink's PKI steering group initiates the correction of deficiencies that may have come to light in the verification operation performed by Samlink's internal audit.

A plan is drawn up to correct deficiencies found in the certifier's own operations, which includes the repair schedules determined based on the severity of the deficiency and the time required for the correction.

If deficiencies have been detected in the activities of the Certifier's subcontractors, those concerned will be informed about them and the subcontractor will be required to correct the deficiencies within a reasonable period of time.

If the inspections result in the need for changes to the Certification Principles or the Certification Policy, the changes will be made and communicated in accordance with section 9.1 "Change Procedure" of each document.

If the Certificate holder or the Relying Party requires a separate audit of the Certificate Service, it is responsible for the costs arising from the audit.

3.8 CONFIDENCE

The confidentiality of personal data concerning certificate holders and the processing of personal and identification data are described in the Certificate Principles in chapter 3.8.

3.9 PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS

Ownership and intellectual property rights are described in the Certificate Principles in chapter 3.9.

3.10 CONTRACTS

The agreements of the various parties of the certificate service are described in Chapter 3.10 of the Certificate Principles.

4 IDENTIFICATION AND AUTHENTICATION

4.1 NAMING POLICY IN THE CERTIFICATION AUTHORITY'S CERTIFICATE

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

The same Certifier's name also appears in the "Issuer" field in all other Certificates issued by the Certifier.

4.2 FIRST REGISTRATION

4.2.1 Naming practices

When registering a new Certificate holder, the information that is stored in the Certificate is defined. This identification information can be found in the Certificate's "Subject" field and "Subject Alternative Name" field.

Naming practices and the use of name parts are described in chapter 4.2.1 of the Certificate Principles.

4.2.2 Name requirements

The name requirements are described in the Certificate Principles in chapter 4.2.2.

4.2.3 Unambiguity of names

The identifier must be unambiguous for all Certificates issued by the Certifier. Unambiguity means that the Certifier does not issue Certificates with identical identifier name values to different devices, applications or programs.

4.2.4 Resolving name ambiguities

Resolving name ambiguities is described in Certificate Principles in chapter 4.2.4.

4.2.5 Proving possession of a private key

When applying for certificates, the Certificate request is submitted to the Certifier electronically signed or confirmed with a one-time ID and password, or with an appropriate document, on the basis of which the origin and legality of the application can be verified and the content of the certificate request on other media can be checked for equivalence.

The certifier verifies that the request came from a source where the Private key corresponding to the Public key to be verified has been available.

4.2.6 Registrant Authentication

The certifier identifies and authorizes the Registration Officers of its own registration point. In registration tasks, the Registration Officers are authenticated with the help of the Certificate.

Only an authorized Registrant can perform registrations.

The certificate principles have a more detailed description of the Registrant's authentication.

4.2.7 Organization authentication

The registrant must ensure the right to use the organization name included in the Certificate in the Certificate.

The certificate principles have a more detailed description of the organization's authentication.

4.2.8 Identification of the certificate holder

The holder of the certificate is represented by the person applying for the certificate, whose authority to apply for the certificate is verified during registration.

The certificate principles have a more detailed description of the identification of the holder of the certificate.

4.3 RENEWAL OF THE CERTIFICATE UPON EXPIRATION

The verified keys that were in use are not re-verified, but new keys are created.

The certificate principles have a more detailed description when the validity expires.

4.4 RENEWAL OF THE CERTIFICATE AFTER EXPIRATION OR CANCELLATION

If the Certificate has been invalidated or its validity has expired, no new Certificate will be created for the keys that were in use. Renewing the certificate requires the creation of new keys.

The procedure for applying for a new certificate is the same as for the first registration.

4.5 CERTIFICATE CANCELLATION OR SUSPENSION REQUEST

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

The person requesting the annulment must be identified in Revocation service. The identification must be done in such a way that the requester's right to request annulment can be verified. Identification mechanisms must take into account the possibility of making unauthorized requests.

The identification method is described in the Certificate Principles.

Only the person in charge of the Revocation Service has the right to submit the Certificate's cancellation request to the Certifier's system. The person charge of revocation is identified based on the Certificate.

4.6 CERTIFICATE RESTORATION REQUEST

The certificate can no longer be restored after revocation.

5 FUNCTIONAL REQUIREMENTS

5.1 APPLYING FOR A CERTIFICATE

Certificate orders and requests must be made and filled in according to the given instructions and must contain the required and correct information.

The certificate principles have a more detailed description of the certificate application procedure.

5.2 ISSUING THE CERTIFICATE

Based on the received electronically signed Certificate Request, Certificate Production creates a Certificate that is signed by the Certifier. The Certifier is responsible for ensuring that the identification information of the issued Certificates is in accordance with the Certificate Request and Registration Information.

The content of the certificate is described in section 8.1 " Certificate profiles ".

In particular, the following matters must be taken care of:

- The procedure for issuing certificates is securely linked to the processes used in key generation and Registration.
- The Certifier must ensure that the unique username of the Certificate holder remains unique in valid Certificates issued by the Certifier.

The integrity of the registration data is protected especially when transferring data between operators of the order process.

5.3 CERTIFICATE ACCEPTANCE

Installing the Certificate on the device or application indicates that the Certificate holder accepts the Certificate and undertakes to comply with the Certificate Principles.

5.4 CERTIFICATE REVOCATION

The Certificate's serial number, revocation time and reason code are published on the Revocation List in the Directory of the invalidated Certificate. The invalidated Certificate is on the Revocation List at least until the end of the validity period indicated on the Certificate.

5.4.1 Circumstances for revoking the Certificate

The certifier can also, by decision of Samlink's Security Department, without a request from the holder of the Certificate, invalidate the Certificate if there is a justified reason for doing so. These reasons include the following:

- The Certifier states that the Certificate has not been issued in accordance with the relevant Certificate Principles or this Certification Policy.
- The content of the certificate involves a dispute regarding the ownership of the name.
- The holder of the certificate essentially violates the agreement made with the Certifier.

5.4.2 The right to request the annulment of the Certificate

However, certificate invalidation can also be initiated with the permission of the Security Department of Verifier Samlink, based on reliable and valid information brought forward by any party, which refers to the invalidation conditions according to section 5.4.1 of this document " Conditions for invalidation of a Certificate " or the corresponding section in the Certificate Principles.

5.4.3 Cancellation request procedure

A certificate cancellation request can be made to Revocation service either:

- by phone (confirmed with a call back if necessary)
- by e-mail, which is electronically signed by the server management person.

All events related to cancellation (request, basis and identification method) must be archived.

Once the Certificate has been permanently invalidated, it can no longer be used.

5.4.4 Cancellation request waiting time

The holder of the certificate is responsible for making sure that the cancellation request is sent to the revocation Service without delay during the service hours of the Revocation Service in circumstances that require this.

The certifier is not responsible for damage caused by unauthorized use of the Private key created for the device or server application.

The certifier is responsible for publishing the revocation information on the Revocation List in accordance with the principles stated in the Certification Principles and Certification Policy.

5.4.5 Publication of the revocation list

The revocation list service is implemented by publishing the Revocation lists electronically signed by the Certifier in a public directory. The integrity of the revocation list is guaranteed by the electronic signature of the Certifier.

The revocation list is published every two (2) hours and is valid for five (5) days. In the event of failure, maintenance and other exceptional situations, a new Revocation List will be published no later than before the expiry of the previous Revocation List's validity period of 5 days. Each Revocation List states the moment of its validity.

The revocation list is available in the Directory 24 hours a day, 7 days a week, except for previously announced maintenance outages. The Certifier is not responsible for the availability of the service, if a fault or interruption occurs in systems or services independent of the Certifier.

There may be several valid Revocation Lists available in the directory at the same time. The most recently published of these contains the most up-to-date information.

5.4.6 Revocation list inspection requirements

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 revocation list information verification procedures are not followed carefully:

- A trusted party that searches the Revocation list from the Directory must verify the authenticity of the Revocation list by checking its electronic signature and the related verification path.
- The relying party must also check the validity period of the Revocation list to make sure that the Revocation list 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 revocation list 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

5.5 RESTORING THE CERTIFICATE TO USE

It is not possible to suspend the validity of certificates, so they cannot be restored for use.

5.6 INFORMATION SECURITY CONTROL

5.6.1 Data to be saved

The Certifier and Certificate Production automatically or manually store the following essential information related to the certification operation:

Information related to the life cycle of the certifier's keys

– generation, backup, recovery and destruction of keys
– maintenance events related to the life cycle of the cryptographic device

Maintenance events related to the life cycle of the Certificates of the Certifier and Certificate holders

– Certificate orders and requests, Certificate renewal requests for new keys
– Temporary closures of contracts
– Certificate revocations
– Creation and publishing of certificates
– Creation and publication of revocation lists. The revocation list is not archived, but the Certificate system is checked after the end of the day to see if all revoked Certificates can be found on the revocation list.

Events related to information security maintenance

– Transactions performed using software tools provided for certificate retrieval
– Measures directed at the certification system or security systems performed by the certification production personnel, e.g. software, hardware and update installations, restores, system shutdowns and restarts, and changes to system settings
– system crashes, hardware failures and other anomalies in systems
– events of routers and firewalls and intrusion detection systems
– access control events to the premises of the verification system.

The recorded data includes the type of data, date and time, as well as the running number of the automatically recorded logs and the identifier of the system that produces the log.

The information mentioned in section 5.4.3 " Invalidation request procedure" is stored in the certifier's revocation service in connection with invalidation requests.

5.6.2 Monitoring of log data

Significant logs related to security and operation are regularly monitored by the staff of Certificate production.

Based on the alarms generated by the systems, the logs are reviewed in order to find out suspicious or abnormal events.

5.6.3 Log data retention period

The log data of the verification system is stored for at least one year after its creation, and after that the data is archived for the period mentioned in section 5.7.2 " Archive storage period ".

Essential log data produced by other systems related to certification are stored in the systems themselves for at least 10 days after they were created. In addition, log data can also be transferred to a separate log server for storage and exported to storage media for archiving.

5.6.4 Log data protection

Manually saved logs as well as logs automatically produced by the Certifier's and Certifier's systems are protected from modification, destruction and unauthorized reading by the systems' access authorization management and access control.

The log data of the verification system is electronically signed.

5.6.5 Log data backup

Backups of the log data of the verification system are taken regularly.

The practice of verifying log data produced by other Certifier and Certificate Production systems depends on the system and the criticality of the log data. The most essential log data are regularly backed up.

5.6.6 Log data collection system

The systems of the Certifier and Certificate Production support the collection of log data. Certain management events for the production system, e.g. system changes and updates, as well as management events related to CA keys, are recorded manually in the physical log.

The log data that is automatically generated in the systems is stored at the application, network device and operating system level. The manual logs are produced as minutes by the staff of Certificate production.

5.6.7 Vulnerability testing of systems

In certificate production, the vulnerability of critical systems is regularly tested in case of intrusion attempts by outsiders. Based on the test results, configurations of firewalls and other systems, as well as operating principles and policies, are updated if necessary.

5.7 DATA ARCHIVING

5.7.1 Data to be archived

Certificate production archives the most critical of the log data described in section 5.6.1 " Data to be saved ", e.g. all logs produced by the verification system, as well as manually generated logs of actions directed at the verification system.

In addition to the aforementioned log information, at least the following information is archived by the Certification Authority or Certificate Production:

- Agreements related to certificate services
- Contracts related to certificate production
- Certificate orders and applications received by the certifier
- Issued Certificates

- Certificate invalidation requests received by the CA's revocation service
- Requests to suspend the validity of Service Agreements received by the Agreement Closing Service
- published revocation Lists
- all versions of the Certification Principles published by the Certification Authority
- all Certification policy versions published by the Certification Authority
- Audit protocols prepared by Samlink's internal audit.

Information can be archived both in electronic form and as physical documents.

5.7.2 Archive retention period

All information mentioned in section 5.7.1 "Data to be archived" will be archived for at least three (3) years from the moment of their creation.

Agreements related to Certificate Service and Certificate Production are kept for at least three (3) years from the date of their expiration.

Published Certificates and their related registration information and Revocation Lists are archived for at least three (3) years from the expiration of the Certificate's validity period.

The Certifier does not guarantee the storage of archives after the Certifier's activities have ended.

5.7.3 Archive protection

The archives, which contain information related to the creation and revocation of Certificates, as well as Certificates and Revocation Lists stored in electronic form, are located in fire-safe premises protected by access control . Information regarding changes to the production system environment of the Certificates is also archived in fire-safe premises protected by access control. Other data to be archived are located in premises protected by at least access control.

5.7.4 Archive backup

Backups of the archive data produced by the verification system are taken in case the data is lost or destroyed, so that if the actual archive is destroyed, the data can be restored from the backups.

5.7.5 Access and review procedures for archival information

Archive data is stored in such a way that only authorized persons of the Certification Authority or Certification Production can access it. Persons who carry out inspections in accordance with section 3.7 " Inspections " are entitled to view archive data. Otherwise, information will only be provided based on a written request within the limits permitted and required by Finnish law and under the supervision of Samlink's Security Department.

The holder of the certificate will be given archival information about himself. The information is provided free of charge within the limits of the inspection right defined in the Personal Data Act. Otherwise, reasonable fees based on workload will be charged for requesting and providing information.

5.8 RENEWAL OF CA KEYS

A new signing key is created for the Certifier at least as long as the lifetime of the longest Certificate issued by the Certifier before the period of use of the existing signing key for signing Certificates ends. The key is used for signing Certificates for a maximum of as long as the validity period of the last Certificate issued with it has expired, before the key's usage period ends. This ensures that the Revocation list can always be signed with the same key with which the Certificates that may end up on it are signed.

The following Certificates are published when the keys are exchanged:

- Certificate signed with the Certifier's new Private key for the Certifier's old Public key
- Certificate signed with the Certifier's old Private key for the Certifier's new Public key
- A Certificate signed with the Certifier's new Private key for the Public key of the same Key Pair.

5.9 DISASTER AND CA KEY EXPOSURE RECOVERY

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

The production system has been duplicated. In case of equipment failure, production is transferred to the backup equipment. In the event of a software failure, the software will be reinstalled. In case of data corruption, the data is restored from a backup, such as is always taken before and after every system change and otherwise regularly. The most critical data is backed up at least 4 times a week. A more extensive destruction of a part of the production system causes a service interruption, the length of which depends on the extent of the problem.

5.9.2 The private key of the certificate authority has been exposed

If the Certifier's Private key is revealed, proceed as follows. Revocation lists signed with this key are removed from the Revocation list service immediately, in which case the Certificates signed with that key cannot be trusted with sufficient grounds. The Certifier informs the holders of the Certificate about the disclosure of the key and provides information about the necessary measures on the intranet pages used by the Certifier and the Banks, as well as by e-mail. The continuation of the operation requires the creation of new signing keys of the Certifier and the creation of new Certificates for the Certificate holders and elements of the information systems.

5.10 TERMINATION OF VERIFICATION ACTIVITIES

The key measures related to the termination of operations are described in the Certificate Principles. The Samlink PKI steering group is responsible for implementing the principles in this regard.

The certifier informs about the termination of its activities as follows:

- Termination of certification activities will be announced on the intranet pages used by the Certifier and the Banks and on the public website
- Any subcontractors handling tasks related to the Certificate Service will be notified of the termination with a letter that also terminates the contract for handling the functions of the Certificate Services on behalf of the Certificate Authority.

In addition, the Certifier takes the following measures in connection with the termination of its operations:

- The certifier terminates the Revocation list service, after which the Certificates issued by it can no longer be justifiably trusted.
- The CA destroys or disables its Private Signing Keys so that they can no longer be used.

6 SAFETY MEASURES

6.1 PHYSICAL SECURITY SOLUTIONS

In the registrant's premises and personnel recruitment, the instructions given on premises and personnel safety are followed.

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

6.1.1 The location and structure of the equipment compartment

The certificate production equipment is located in Finland in premises whose physical protection meets TRAFICOM/54045/03.04.05.00/2020, order on securing communication networks and services and synchronization of communication networks, protected according to importance class 1.

6.1.2 Physical access control

Unauthorized access to the premises where the equipment used in the production of the Certificate Service is located is blocked. In addition to our own personnel, only the maintenance staff and cleaners of the various equipment can enter the equipment premises, and even then only after they have proven their identity and the necessity of their visit. If the person has not been granted a permanent personal access right, he can only move around the premises in the company of a person entitled to access.

The flow of staff members visiting the equipment rooms is organized in such a way that everyone has access during their own working hours only to those rooms where they need to stay due to their work duties. Personnel visits are regularly monitored from the log data of the access control system.

Access control to premises with security is arranged in such a way that no one can enter there without leaving an entry in the access control system.

6.1.3 Electricity supply and air conditioning

Uninterrupted operation of the verification system is ensured by means of an uninterruptible power supply system and backup power devices. The equipment rooms have an air conditioning system, the temperature and humidity of the air it produces is monitored.

6.1.4 Protection against water damage

The device status is monitored with humidity detectors. The equipment rooms have a raised floor and a drainage system in case of water leaks.

6.1.5 Fire safety

The equipment premises are covered by an automatic fire alarm system. The premises are equipped with fire detectors. In addition, a first firefighting team is maintained in case of emergencies.

6.1.6 Storage of information material

Data media on which information related to or generated by the Certificate production system is stored are stored in the same secure facilities where the system itself is located. See also section 6.1.8 " Safety copies stored elsewhere ".

6.1.7 Disposal of waste material

The discs, magnetic tapes and installation disks of the certification system with their backups, which are not permanently stored in the production facilities of the Certificates, are safely disposed of when they are no longer needed.

6.1.8 Backup copies stored elsewhere

Backups are taken of the log data produced by the certification system, which are stored in facilities located separately from the Certifier's production facilities. The protection of these facilities is at the same level as the protection of the Certifier's production facilities.

6.2 FUNCTIONAL SECURITY SOLUTIONS

6.2.1 Trusted managers

Trusted managers have the following responsibilities:

- Information security officer: overall responsibility for managing the implementation of security practices
- System administrator: Configuration, maintenance and installation orders of the Certifier's trusted systems related to the creation of certificates, revocation of certificates, as well as troubleshooting and procedures for managing the Certifier's private keys
- System manager: Daily monitoring of the use of the certifier's reliable system, taking backups, implementation of the backup system and management of recovery, as well as installations according to orders and troubleshooting on the system level
- System reviewer: Maintaining and checking archives and audit logs of the certifier's trusted systems
- Registration officer: Collecting and registering the information needed to create certificates
- Certifier's closing service manager: Approval of measures related to the invalidation of certificates and the Revocation List.

- Trusted task managers are placed in the tasks that are the responsibility of the various parties of the verification operation as follows:

Trusted manager	**The party to the verification activity**
Information security officer	Certifier, Certificate production
System administrator	Certificate production
System manager	Certificate production
System Evaluator	Certifier, Certificate production
Registration officer	The holder of the service contract
The certificate's revocation service manager	Certifier
Contract closing service manager	The external operator responsible for the security service

Persons acting in trusted roles undertake to comply with this Authentication Policy.

6.2.2 The number of persons required for the tasks

The certifier ensures that sufficient personnel have been hired for each task and that individual persons cannot act in all roles at the same time.

Certain procedures require the simultaneous participation of several people. Implementing changes and backing up and restoring the Certifier's private key to the Certifier's production system environment requires the participation of at least two people. The creation of the Certifier's Private key requires the presence of at least four people.

6.2.3 Identification and authentication of trusted agents

A Certificate is required to identify the following operators:

- System administrator
- The certificate's revocation service manager

As a rule, a username and password are used to identify the administrators listed below. When performing the duties of the entrusted activity requires the use of the Certifier's most critical systems, logging into these also requires identification based on the Certificate from those acting in the roles listed below.

- Information security officer
- System manager
- System Evaluator

6.3 PERSONAL SAFETY

6.3.1 Background check procedure

A background check is carried out for the following managers:

- Information security officer
- System administrator

Otherwise, the Certifier and any subcontractor responsible for Certificate production will check the background information of their employees at their discretion, depending on the employee's role in the production of Certificate Services.

6.3.2 Educational requirements

New employees of the Certifier and any subcontractor responsible for Certificate production are familiarized with the certification operation in general, the security requirements related to it, and their own work tasks in particular. The material to be processed includes e.g. information security principles, Certificate principles and Certification policy. If necessary, individual orientation and training tailored to the person's work tasks and role will be arranged.

Further training is organized for employees if necessary.

6.3.3 Consequences of unauthorized actions

If the Certifier or a possible subcontractor responsible for Certificate production discovers misconduct, the employee who committed it will be immediately transferred to other tasks and all his access rights to systems related to certification activities will be revoked. Regarding follow-up measures, the valid practices of the Certifier and the relevant subcontractor are followed.

6.3.4 Contract worker requirements

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

7 TECHNICAL SECURITY SOLUTIONS

This chapter contains the requirements of the Public and Private key management principles and related technical control, which apply to the Certifier, a possible subcontractor responsible for Certificate production, other possible subcontractors and Certificate holders.

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

7.1.1 Creating a CA Key Pair

The Certifier's Key Pair is created in accordance with the key generation procedure approved by the Certifier. The key pair is created in the physically protected premises of Certificate Production using the certification system in a high-security HSM device (see section 7.1.6 " Protecting the Certifier's Private Key "). The persons participating in the key generation are trusted administrators who are authorized for this task and at least two of whom must be present. In addition, at least two supervisors authorized by the Certification Authority must be present. The steps of the key creation procedure are recorded in the protocol, and each person participating in the procedure confirms the protocol with their signature. The minutes are stored in accordance with section 5.7 " Data archiving ".

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

The Certifier's Public Key is available on the intranet pages used by the Certifier and the Banks, as well as on the public website, where the Certificate of the Certifier's Public Key signed by the Certifier itself is published, as well as the Certificate's summary, the so-called fingerprint.

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

The certifier uses a signature key based on the RSA algorithm, the length of which is at least 4096 bits, to sign Certificates and Revocation list data.

7.1.4 Lifetime of the Certifier's Key Pair

The lifetime of the Certifier's Private key is at most twenty-five (25) years. The useful life cannot be longer than the validity period of the Certifier's Certificate associated with the key. If the Certificate holder's Certificate is invalidated, the Revocation list is signed with the same key used to sign the Certificate in question. The key must be able to be used during the validity period of the related Certificate to invalidate the Certificate of the last Certificate holder signed with it throughout the validity period of this Certificate. The key can therefore be used to sign the Certificates of the Certificate holders for the lifetime of the key, 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.

7.1.5 Purposes of the certifier's keys

The Certifier's signing keys can only be used in the Certifier's physically protected premises under the supervision of trusted agents using the certification system and the HSM device defined in section 7.1.6 " Protection of the Certifier's Private Key ".

The purposes of use of the Certifier's Public Key, which are indicated in the "key usage" field of the Certifier's Certificate, are:

- keyCertSign (Checking the Certifier's signature on Certificate holders' Certificates)
- CRLSign (checking the signature of the revocation list information published by the CA).

NOTE The Certifier can use its signing keys to issue Certificates also as a root certifier, in which case the holder of the issued Certificate is another Certifier.

7.1.6 Protecting the Certificate Authority's Private Key

Certificate production has implemented the protection of the Certifier's Private Signing Key with a combination of physical protections, defined procedures, access control and user rights.

The certification system, which is located in safe, physically protected premises, includes an HSM device (Hardware Security Module), with which the Certifier's signing key is protected. The HSM device complies with at least the FIPS 140-3 standard.

With the help of technical supervision and defined procedures, Certificate production makes sure that no one alone gets the means to access the environment where the Private Key is stored, or is able to use the key in any way. Critical procedures related to the signing key, such as key storage, verification and recovery, are always performed by more than one person.

The return of the key requires the use of activation information that is stored divided into parts in separate secure spaces and access to which is distributed to the number of trusted administrators specified by the Certifier. Returning the key requires that at least two trusted administrators and two supervisors authorized by the Certifier participate in the return procedure.

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

Key escrow-type copying and storage is not performed for the Certifier's Private key under any circumstances.

7.1.8 Backing up the private key of the CA

In the event that the Certifier's Private Signing Key is destroyed, there is an arrangement for its recovery. The private key of the CA must be in encrypted or shared form in the backups. During the physical processing of the backup copies, two trusted managers of the Certificate Production must be present.

7.1.9 Archiving of the CA's Private Key

The private key of the certificate authority is not archived.

7.1.10 Activation of the private key of the certificate authority

The activation of the Certifier's Private key is included in the procedure according to section 7.1.1 " Creating the Certifier's Key Pair ". Activation takes place by a trusted administrator after the verification system has identified the administrator with a strong identification mechanism. The key remains active in the verification system until its use is interrupted, e.g. due to maintenance procedures.

7.1.11 Deactivation of the private key of the certificate authority

The Certifier's Private key can be deactivated by a trusted administrator.

7.1.12 Destruction of the Certificate Authority's Private Key

When the use of the Certifier's Private key is terminated, all copies of it are destroyed or stored in such a way that their use is prevented.

7.1.13 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 takes care of the creation of the Key Pairs related to the ordered Certificates with its own components and in accordance with the security level offered by these components.

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

The holder of the certificate is responsible for the safe delivery of the Public key used by the device or server application to the Certifier.

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

The length of the keys used in connection with the RSA algorithm used by certificate holders is at least 2048 bits.

7.2.4 Lifetime of the certificate holder's Key Pair

The validity period of the Certificate determines the lifetime of the Certificate holder's Public and Private keys, which is a maximum of two (2) years. Keys are not recertified when the validity period of the related Certificates is about to expire.

7.2.5 Purposes of the certificate holder's keys

The private keys of the certificate holder can only be used for purposes that correspond to section 8.1 of the relevant Certificate Principles. Purposes of Public Keys mentioned in the "Certificate Profiles" tables.

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 Archiving of the certificate holder's Private Key

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

7.2.8 Destruction of the private key of the certificate holder

The holder of the certificate takes care of the destruction of Private related to the certificate after the end of the life cycle of the certificate.

7.2.9 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 requirements of the Certifier's information security principles are followed in maintaining the information security of information systems.

7.3.1 Security classification of information systems

In the security classification of certificate production systems, the multi-level information system security classification policy defined by the subcontractor responsible for certificate production is followed.

7.3.2 Information system user identification and access control

Access control takes care of identifying different trusted agents before accessing the systems (see section 6.2.3 " Identification and authentication of trusted agents "). The systems also provide traceability of actions taken by different users.

7.3.3 Procedures that require the participation of several people

Carrying out certain procedures related to the certification system requires the participation of several people (see section 6.2.2 " Number of persons required for tasks ").

7.3.4 Capacity control

The use of the system's resources is constantly monitored and the automatic monitoring system gives an alarm when the set limits are exceeded.

7.3.5 Requirements related to information security monitoring

The requirements related to the information security of the certifier's systems and operations are described in section 5.6 " Information security control ".

7.3.6 Management of exceptional situations

Reporting procedures and action plans have been defined for various exceptional situations.

7.3.7 Data security requirements

The storage, archiving and processing of data that has become unnecessary is described in sections 6.1.6 " Storage of data" and 6.1.7 " Disposal of waste material ".

7.4 LIFECYCLE MANAGEMENT SECURITY SOLUTIONS

7.4.1 System development management

A separate testing environment is used in system development for certificate production, where the changes resulting from the development work are tested before they are exported to the production system.

All system changes that are brought into production are carefully documented.

7.4.2 Information security management

7.4.2.1 Information security maintenance

In all its activities, the Certifier complies with the information security principles, the Certification Principles and this Certification Policy. Operational inspections are described in section 3.7 " Inspections ".

The certifier ensures, through contracts, that information security is maintained with regard to outsourced functions and that the defined principles and practices are followed when using subcontractors.

7.4.2.2 Resource management

The certifier and any subcontractor responsible for certificate production follow the information security principles they have drawn up in protecting the resources they use and the information they produce and use.

7.4.2.3 User service management

The management of the user service is based on the implementation of the information security principles of the Certifier and any subcontractor responsible for the production of the Certificate, compliance with the prepared instructions and the implementation of the responsibilities defined in the contracts with the subcontractors, as well as the monitoring of the activities required by the information security principles, instructions and responsibilities.

7.4.2.4 System access control

Information security principles and defined practices are followed in the management of user rights and access control of the Certifier's and Certificate Production systems. The management of user rights for different systems is handled separately by persons authorized for this task.

7.4.2.5 HSM device lifecycle management

Certificate production has prepared an instruction on the life cycle management procedure of the HSM device used for signing Certificates and Exclusion Lists in order to implement the requirements defined in the Certificate Principles.

7.5 TELECOMMUNICATION NETWORK SECURITY SOLUTIONS

The authentication system is separated from the public network by firewalls. The most critical parts of the system are completely isolated from the public network. An attack detection system is also in use.

Traffic between parts of the certifier's system uses strong identification and encryption.

8 CERTIFICATE AND REVOCATION LIST PROFILES

8.1 CERTIFICATE PROFILES

All Certificates issued in accordance with these Certificate Principles 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 certificates comply with version 3 of the X.509 standard and use the following certificate extensions defined in the standard:

- Authority key identifier of the certifier
- Public key identifier of the certificate holder (Subject key identifier)
- CRL distribution points
- Extended key usage

The X.509 standard also allows self-defined certificate extensions. Certificates do not use private certificate extensions.

A certificate extension is defined as critical when the system using the Certificate is to reject the Certificate if it does not recognize the extension defined as critical. None of the extensions mentioned above are defined as critical.

An official identification number (OID) has been applied for the Certificate Principles and there is a reference to the Certificate Principles in the Certificate.

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
Place of publication of the revocation list	CDP CRL distribution points	URL= http://httpcrl.trust.telia.com/samlinkcustomerca.crl
Key purpose extension	Extended key usage	critical Digital Signature, Certificate Sign, CRL Sign

8.2 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 revocation list	Effective date	CRL creation time
Publication time of the next Revocation 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 MANAGEMENT OF THE CERTIFICATION POLICY

9.1 CHANGE PROCEDURE

Whenever changes are made to the Certification Principles or new Certification Principles are written, the effects of the new requirements on the Certification Policy are evaluated. Samlink's Security Department is responsible for starting the evaluation. There may also be other reasons for changing the document independent of the changes related to the Certificate Principles. 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 take effect immediately after it has been approved and the change has been entered into the Certification Policy. A major change is notified at least 15 days before its entry into force to those whose operations it affects.

9.2 APPROVAL PROCEDURE

All changes to this Verification policy, except changes related to appearance, spelling or contact information, must be approved by the Samlink PKI control group.

9.3 PUBLICATION

The verification policy is made available to those parties who are required to comply with it.

The verification policy is published for the parties who are required to comply with it, on the intranet sites used by Samlink and the banks, on the public website or in another separately agreed way.

Also the previously valid versions of the Certification Policy are available from the aforementioned addresses at least until the end of the life cycle of each Certificate issued according to the Certification 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.