TELIA MOBILE ID CERTIFICATE

CERTIFICATION PRACTICE STATEMENT

(Translation from official Finnish version)

Version 2.3

Valid from June 30, 2017

Telia Finland Oyj, domicile: Helsinki, Teollisuuskatu 15, FI-00510 Helsinki, tel. +35820401, business ID 1475607-9, ALV reg.

Contact information

The organisation managing the Certification Practice Statement

This Certification Practice Statement is managed by Telia Finland Oyj's (later: Telia) Certificate Policy unit,

Contact information for Telia:

TELIA FINLAND OYJ
00051 TELIA
Tel: +358 (0) 20401

The contact person on issues related to the Certification Practice Statement:

Telia CA Product Manager
Email: cainfo@telia.fi
Tel: +358 (0) 20401

Telia owns the immaterial rights of this Certification Practice Statement.

Customer Service and Revocation Service

The use of the Mobile Certificate can be blocked through Telia's Revocation Service. This may be announced:

by calling the operator's customer service: +358 20 017 000 (open working days from 8:00 AM to 8:00 PM and Saturdays from 9:00 AM to 4:30 PM)
by calling the operator's technical customer service: +358 20 690 101 (open 24 hours a day, 7 days a week)
At the operator's authorised customer service points and at the dealers' locations during opening hours

The Certification Practice Statement's identifiers

The name of this Certification Practice Statement is **"Telia Mobile ID Certificate, Certification Practice Statement"**.

This Certification Practice Statement describes how Telia is implementing the Mobile Certificate Service's identity federation's joint Certificate Policy : "Mobiiliasiointivarmenne – Varmennepolitiikka" (Mobile Transaction Certificate - Certificate Policy".

The object identifiers of this Certification Practice Statement are:
1.2.246.277.1.11.4.1.2.1 (issued 2010-2011)
1.2.246.277.1.11.4.1.2.2 (issued 2011-02/2016)
1.2.246.277.1.11.4.2.2.3 (issued from 02/2016)

Version management

Version	Date	Description
1.0	November 30, 2010	The first approved and published version
1.0.1	December 20, 2010	Added the address for the CA revocation list. Fixed spelling errors
1.0.2	June 6, 2011	New Telia logo
1.0.3	November 4, 2011	Added the creation of the first key pair using a card (6.1.1.2)
2.0.0	February 1, 2016	Added a new encryption algorithm
2.1	December 1,2016	Fixed and cleared several small issues, this English translation
2.2	March 23, 2017	Sonera -> Telia
2.3	June 30, 2017	Identification documents

Concepts and terms related to this subject

The term used in this document	Description
Activation Data	A PIN code or password, which protects the use of a private key, and which can be entered to activate it. The Mobile Certificate's private keys are located on the phone's SIM card.
Subordinate CA	A Certification Authority, whose certificate has been signed by the Root CA and who grants certificates for end entities it has defined itself
Signature Creation Data	An unique information entity used by the signing party in creating an electronic signature, such as a code or private key
Transaction Certificate	A transaction certificate is a certificate in accordance with the Act on Strong Electronic Identification and Trust Services (617/2009). A Transaction Certificate is not necessarily the quality certificate indicated in this Act.
Digital Signature	An electronic signature made using the private key of the document's or message's signer, in accordance with the public key method. Generally, the signature is an encrypted digest of the message.
Elliptic Curve Cryptography	An asymmetric encryption algorithm, used to create an asymmetric key pair.
Directory Service	In a public key system, a service containing user certificates and other possible related information, as well as directories containing Certificate Revocation Lists. Usually maintained by the Certification Authority itself.
Public Key	A public part of an asymmetric key pair, used in the encryption techniques of the public key method. The public key is contained in the certificate that the Certification Authority publishes in its Directory Service.
Public Key Infrastructure (PKI)	A system enabling the use of the public key method, where the Certification Authority certifies the public part of a key pair with its digital signature and distributes these certificates to other users, maintains
	a directory of public keys and a Certificate Revocation List, and possibly offers other services related to the use of the system.

Public key method	An asymmetric encryption method, where each user has two keys that are connected to each other. One key in the key pair is the public key, which is published in the public directory, and the other is a private key held only by the key pair's user. The information encrypted using a private key may be opened only using the matching public key, and vice versa.
Root CA	In a public key system, the highest trusted party, which signs, distributes, and, when necessary, cancels the certificates of the lower-level Certification Authorities.
nonRepudiation	One of the key's purposes of use, used to make an advanced electronic signature, made using the mentioned key, contractually binding under law. The nonRepudiation key enables the signing of the agreements. When signing a document using a nonRepudiation key, it is possible to verify the document's integrity and authenticity using a certificate matching the key in question. See *Electronic signature* below.
Subscriber Identity Module (SIM)	The card to which the telephone subscription has been bound. In spoken language, this is usually called the SIM card.
End Entity	The person to whom the Certification Authority has granted the certification. The end entity uses the certificate and legally possesses the private key matching the public key contained by the certificate, as well as the PINs needed to use it.
Relying Party	The party offering electronic services for the end entities. The Relying Party relies on the certificate in their operations and/or verifies the digital signature using the certificate.
Trust Anchor	The certificate that the Relying Parties define as the top of their certificate hierarchy. The Relying Parties have to trust the certificates below it.
Mobile Certificate	A Mobile Certificate or mobile ID certificate is a

	Transaction Certificate, based on private keys located on the SIM cards of a mobile device. A Mobile Certificate in accordance with this document can be used for the electronic identification of a person, the encryption of communications, and for electronic signatures. The Mobile Certificate can be used, according to its purpose of use, for administrative applications and services, and the applications and services offered by private organisations (Relying Parties). In this document, for easier readability, the term Mobile Certificate is capitalised, unless the context requires otherwise.
Mobile Transaction Certificate	Same as Mobile Certificate
Registration Authority (RA)	The party responsible for authenticating the Certificate Applicant and verifying the information registered to the certification application. The Registration Authority operates as a part of the a certification organisation, authorised by the Certification Authority
RSA	An asymmetric encryption algorithm, used to create an asymmetric key pair. The abbreviation comes from its inventor's surnames: Riest, Shamir, and Adleman.
Certificate Revocation List (CRL)	In a public key system, a list of certifications that have been removed from use. The Certification Authority publishes a Certificate Revocation List in the Directory Service.
Consent	The validation of a transaction or an operation using a key with the purpose *digitalSignature* but not the purpose *nonRepudiation*.
Electronic signature	A personal signature or an equivalent, in a format readable by a computer, such as a digital signature. The electronic signature serves as proof of a connection between the signature-related document or message and a specified person. In spoken language, an electronic signature generally means a digital signature that has *nonRepudiation* as one of the purposes of use of the key that has been used to make it.
Authentication; Verification	Confirming the identity of a system user (person, organisation, or device) or, in communication, the other party.

Identification	Identifying the other party in transactions. At its most simple, an event where the other party answers the question "Who are you?"
Tool of identification	A SIM card with private keys and the related PINs.
Validation	Proclaiming the correctness of the certificate, an operation performed using the certificate, or its final result.
Certificate	A certificate is an item formed by a person's public key, name information, and other information included in the certificate, which the Certification Authority has signed using its own private key. The certificate's authenticity can be verified by checking the Certification Authority's Digital Signature.
Certificate Application	A Certificate Application is a form completed by the Certificate Applicant, which contains the Certificate Applicant's personal, organisational, and contact information. The form is approved by the application's approver and, when necessary, a trusted person.
Certificate organisation	The parties of the certification organisation include the CA, the Registration Authority, the card manufacturer, the producers of directory and Certificate Revocation List services, and all other service producers whose services are used by the Certification Authority of the service.
Certificate service	The certificate service is a certificate-based identification and signature service, utilised by the Relying Party for the services they offer for Certificate Owners.
Certificate Policy	A named group of rules that form the basis that makes it possible to evaluate the certificate's suitability for a certain purpose, the general requirements for security policy, and other such requirements. **Certificate Policy** *(CP)* is a description, created by the CA, of operations and operating principles that are applied when granting certificates. The Certification Practice Statement describes the Certification Authority's operations in more detail than the Certificate Policy.

Certificate Path	The [logical] chain of certificates from the end entity's certificate to the Root CA's certificate, required to confirm the certificate's origin.
Certificate Request	A Certificate Request is a digital request to form and publish a certificate, sent to the Certification Authority, formed by the Registration Authority, and based on a Certificate Application.
Certification Practice Statement (CPS)	A detailed assessment of the operating methods used by the certificate organisation in approving and managing certificates. The Certification Practice Statement describes how the Certification Authority implements its Certificate Policy, and also describes, in detail, the practices and the methods of operation followed by the Certification Authority. The structure of the Certificate Policy and the Certification Practice Statement mainly follow the division set in IETF RFC 3647 [RFC3647].
Certification Authority (CA)	The certification organisation's party that grants certificates by signing the certification information with its own private key.
Private Key	An encrypted part of an asymmetric key pair, used in the public key's encryption techniques. A private key is typically used for signing documents digitally or opening messages encrypted with a public key. The concept of a "secret key" is also often used in spoken language. The Certificate Owner's private keys have been saved on a SIM card to protect them from unlawful use.

Abbreviations

Abbreviation	Description	The meaning used in this document
ARL	Authority Revocation List	A Certificate Revocation List published by the Root CA, containing information on certificates issued by Certificate Authorities and removed from use.
CA	Certification Authority	Certification Authority (CA)
CP	Certificate Policy	Certificate Policy

CPS	Certification Practice Statement	Certification Practice Statement (CPS)
CRL	Certificate Revocation List	List of invalid certificates
ECC	Elliptic Curve Cryptography	An encryption method based on elliptic curves
HSM	Hardware Secure Module	A special device used for creating and storing Certification Authorities' keys
ICCID	Integrated Circuit Card Identifier	The unique serial number of a SIM card
IETF	Internet Engineering Task Force	An international community advancing the technological development of the Internet
MSISDN	Mobile Subscriber ISDN Number	The mobile phone's phone number
MSSP	Mobile Signature Service Provider	The service platform enabling the making of signatures on a mobile phone, as well as their verification.
OCSP	Online Certificate Status Protocol	Real-time certificate revocation information protocol
OID	Object Identifier	Certificate policy's identifying information
PDS	PKI Disclosure Statement	An individualised description of the conditions and limits of using the certificate.
PIN	Personal Identification Number	Personal code to protect keys
PKI	Public Key Infrastructure	The public key's certificate system
PKIX	-	IETF PKI task force
PUK	Personal Unblocking Key	PUK code
RA	Registration Authority	Registration Authority (RA)
RSA	Rivest, Shamir ja Adleman,	Encryption algorithm
X.509	-	The standard defining the structure of the certificate and the Certificate Revocation List

Roles

Subscription Orderer	Responsible for the payment of invoices. A natural person or a company that allows the subscription's services. May be the same as the subscription user.
Subscription User	The user of the subscription and the services. A natural person who has been marked as the owner of the subscription. The user may be the same as the subscription orderer.

Certificate Applicant	Always the same natural person as the subscription user. A Certificate Applicant must be marked as the owner of the subscription.
Certificate Owner	A natural person who has been granted a Mobile Certificate. Always the same natural person as the certificate applicant, meaning the subscription user.

1 Introduction

1.1 Mobile Certificate Service

The Finnish telecom operators have jointly implemented a Mobile Certificate Service. This service can be utilised by all consumers using mobile phones in Finland to securely visit the various electronic services of the service producers. Telia Mobile Certificate is a certificate service for Telia's mobile customers.

Telia Mobile Certificate is a service in which a strong electronic identifier, or a certificate, is included in the SIM card of the customer's mobile phone. If a mobile phone is equipped with a certificate and a supporting SIM card, it may be used as a identification and signature tool for various transaction and communication services.

Telia Mobile Certificate offers users an easy and secure way to provide identification in all the services that support mobile certificates, and to confirm the contents and the non-repudiation of their commitments. National electronic personal ID (FINUID) in the certificates is used as the identifying information of the Telia Mobile Certificate users. This code and related personal names are always verified from database of Finnish Population Register Center.

The Telia Mobile Certificate is based on X.509 certificates and public key Infrastructure, where the certificate-related private keys are on a SIM card, protected with a PIN. Using the Telia Mobile Certificate Service's signature certificate, the user can perform advanced electronic signatures that are based on the public key method, an RSA or ECC algorithm, and at least 1024-bit (RSA) or 256-bit (ECC) information security keys. All new keys since 02/2016 are based on ECC algorithm.

The deployment of a Telia Mobile Certificate may require the replacement of the SIM card. The user must take particular care to ensure that the mobile phone and the PIN of the Telia Mobile Certificate cannot be used by other parties.

1.2 Certification Practice Statement (CPS)

The Certification Practice Statement is the Certification Authority's description of the practices it follows in granting certificates. The intent of this Certification Practice Statement is to describe the methods used by Telia's Certification Authorities, Teliasonera Mobile ID CA v1, and Teliasonera Mobile ID CA v2, when they grant mobile certificates for natural persons who have a customer relationship with Telia. When granting Telia's mobile certificates, the practices documented in the more generic Certification Practice Statement "Teliasonera Production CPS" are also followed. This statement can be found from the public link https://repository.trust.teliasonera.com/CPS. It describes all the common security arrangements and practices affecting all the certificates granted by Telia. If that statement contradicts this document, the practices of this document are followed.

The Certificate Policy steering the implementation and maintenance of the Certification Authority's services, and defining the rules for applying for certificates, their granting process, and their use, has been described in the Mobile Certificate Service's identity federation's common Certificate Policy "MOBIILIASIOINTIVARMENNE – Varmennepolitiikka" (Mobile Certificate - Certificate Policy).

The Certification Practice Statement follows the structure of the Certificate Policy.

1.3 Mobile Certificate

The Mobile Certificates can be used for identification, encryption, and confirming the integrity, confidentiality, and non-repudiation of data or an event. Mobile Certificates are private-key-based certificates that are located on a mobile end device's SIM card and that have been granted by a Certification Authority belonging to an identity federation. All the Certification Authorities belonging to an identity federation are independent, and all Certification Authorities have their own Root Certificates, which are trusted by the users of the certificates. The certificate-granting process always requires an agreement between the Certification Authority and the certificate applicant.

1.4 Certification organisation

1.4.1 Certification Authority (CA)

The Certification Authority operating in accordance with this Certification Practice Statement is Teliasonera Finland Oyj. The Certification Authority's identifying information can be found in the *Issuer* field of each granted certificate. Telia's mobile certificates are granted by the Certification Authorities "Teliasonera Mobile ID CA v1" (RSA based certificates) and "Teliasonera Mobile ID CA v2" (ECC based certificates).

The Certification Authority's certificates have been granted and signed by Telia's Root CA "Teliasonera Root CA v1".

The Certification Authority produces the certificate service and is responsible for it as an entity. The Certification Authority creates the end entity's certificates and Certificate Revocation Lists, and signs them using the Certification Authority's private key.

1.4.2 Registration Authority (RA)

The Registration Authority is the party that is commissioned by the Certification Authority for operations, for which the Certification Authority is responsible, and that manages the practical work related to the Certificate Applications, in accordance with the Certificate Policy and the Certification Practice Statement. The Registration Authority's tasks include recognising the certificate applicant and approving their application.

The authorised parties operating as the Registration Authorities of the Mobile Certificate are the local customer service points and the dealers. The certificate applicant may apply for a certificate using Telia's self-service portals. In these cases, the Certification Authority's registration system operates as the Registration Authority.

1.4.3. The issuer of the SIM card

The issuer of the SIM card operates as commissioned by the Certification Authority and as the Certification Authority responsible for the key pairs and activation data connected to the mobile certificate. The issuer of the SIM card delivers the customer and card information needed to register the mobile certificate to the subscription user and the Certification Authority.

The issuers of the SIM card are Teliasonera Finland Oyj's mobile operators Telia and Tele Finland.

1.4.4 Revocation Service

The Revocation Service closes certificates that the certificate's owner, the Certification Authority, the Registration Authority, or the card's issuer want closed before the end of the certificate's validity period. Telia's customer service operates as the Revocation Service. The Revocation Service's contact information can be found in the chapter "Contact information", at the beginning of the Certification Practice Statement.

1.4.5. Directory Service

The Directory Service is a service intended for the parties trusting the certificate, which can be used to find out the Certificate Authority's certificate policies and Certification Practice Statements, certificates, Certificate Revocation List (CRL), and revocation information (OCSP), as well as mobile certificates. Some of the Directory Service's information is publically available, and some is only available to the Certification Authorities and the service producers trusting the Mobile Certificate in accordance with chapter 2.1 "The publication and availability of the data".

1.4.6 Certificate Owner

The certificate owner is a natural person to whom the Certification Authority has granted a mobile certificate in accordance with their Certification Practice Statement.

1.4.7 The Relying Party of the certificate

The Relying Party of the certificate is a person or an organisation that relies on the information on the certificate and that uses the certificate to verify the identity of the certificate owner or an electronic signature made by the certificate owner.

1.5 Security arrangements

The security arrangements follow the definitions in the document "Teliasonera Production CPS", which is available at

http://repository.trust.teliasonera.com/

1.6 Using the certificate

The mobile certificate can be used for a person's electronic identification and to offer electronic signatures. The mobile certificate can be used in various applications and services, whose service provider has made an agreement with the Certification Authority.

1.7 The responsibilities and obligations of the parties

The identity federation of the Mobile Certification Service is formed by Certification Authorities who have made a mutual agreement on the production of the services. On the basis of the agreement it has made, the Certification Authority has committed to following the Mobile Certificate Service's identity federation's common Certificate Policy.

The Certification Authority holds the full liability for the certification service. The Certification Authority is responsible for the following attributes applying to the certificates that have been granted in accordance with the Certificate Policy and this Certification Practice Statement:

- The Certification Authority has granted the certificate and manages it in accordance with the Certificate Policy and this Certification Practice Statement.

- The information registered for the certificate owner has been entered on the certificate correctly
- The Certification Authority's private keys have been saved on a secure device
- The Certification Authority's certificate and the up-to-date revocation information are available from the Directory Service 24 hours a day, 7 days a week

All of the Certification Authority's operations follow the currently valid legislation, Certificate Policy, and Certification Practice Statement.

The Certification Authority can use other parties to produce the certification services. In the agreements it has made with other parties, the Certification Authority requires them to follow the practices, responsibilities, and duties required in the Certificate Policy and the Certification Practice Statement.

The responsibilities and duties of the different parties of the certification organisation are described in Annex 1, "The responsibilities and obligations of the certification organisation".

The responsibilities and duties of the parties are agreed in more detail in the agreements between the Certification Authority and the service providers, and the Certification Authority and the certificate applicant.

2 General terms and conditions

2.1 The publication and availability of the data

2.1.1 Publishing the Certification Authority's information

2.2 Telia Mobile ID CA v1

The Certificate Revocation Lists are commonly available in the Certification Authority's LDAP directory and on their website.
The Mobile Certificate Service's Certificate Revocation List is found at the following addresses:

- **ldap:**//crl-1.trust.teliasonera.com/cn=Teliasonera%20Mobile%20ID%20CA%20v1, o=Teliasonera,c=fi?certificaterevocationlist;binary
- **http:**//crl-3.trust.teliasonera.com/teliasoneramobileidcav1.crl

The Certification Authority's certificate's Certificate Revocation List is found at the following addresses:

- **ldap**://crl-1.trust.teliasonera.com/cn=Teliasonera%20Root%20CA%20v1, o=Teliasonera?certificaterevocationlist;binary
- **http**://crl-2.trust.teliasonera.com/teliasonerarootcav1.crl

The mobile certificates are available to the Certification Authority in the Certification Authority's own databases.

The following information on the Certification Authority and the certificate service are publically available on the Internet at https://repository.trust.teliasonera.com

- the valid Certificate Policy (CP) and its previous published versions
- the valid Certification Practice Statement (CPS) and its previous published versions
- a description of the file in accordance with the Personal Data Act.
- the certification authority's certificates

2.3 Telia Mobile ID CA v2

The Certificate Revocation Lists are commonly available on the Certification Authority's websites. The Mobile Certification Service's Certificate Revocation List or revocation information is found at the addresses

- http://crl-3.trust.teliasonera.com/teliasoneramobileidcav2.crl
- http://ocsp.trust.teliasonera.com

The Certification Authority's certificate's Certificate Revocation List is found at the following addresses:

- http://crl-3.trust.teliasonera.com/teliasonerarootcav1.crl
- http://ocsp.trust.teliasonera.com

The mobile certificates are available to the Certification Authority in the Certification Authority's own databases.

The following information on the Certification Authority and the Certificate Service is publically available on the Internet at https://repository.trust.teliasonera.com

- the valid Certificate Policy (CP) and its previous published versions
- the valid Certification Practice Statement (CPS) and its previous published versions
- a description of the file in accordance with the Personal Data Act.

- the certification authority's certificates

2.4

2.4.1 The frequency of publication of the Certificate Revocation Lists

The Certificate Revocation Lists are published at least hourly and are valid for 24 hours from the moment of publication. The Certificate Revocation List is always updated immediately after a change. The Certification Authority's OCSP service offers up-to-date revocation information.

2.4.2 Availability of information

The Certificate Revocation List and OCSP revocation data are available in the Certification Authority's directory to all those that need them. They are available 24 hours a day, 7 days a week, apart from necessary maintenance breaks. The Certification Authority is not responsible for any user-experienced service availability, when the fault or interruption is due to systems or services that do not depend on the Certification Authority.

The certificates are published in a directory that can only be accessed by the Certification Authority's systems.

The Certificate Policy and Certification Practice Statement are publically available documents, distributed on the Certification Authority's website.

2.4.3 Data storage

The information published by the Certification Authority is available on the Certification Authority's website. The certificates are saved in the Certification Authority's confidential data storage. The Certification Authority's information is archived in accordance with the Certificate Policy's requirements and this Certification Practice Statement.

2.5 Audit

2.5.1 Inspections performed by the Certification Authority itself

The Certification Authority monitors the certification system's log information by monitoring the compliance and the data security of its own locations, systems, and operations using random inspections, as well as those of their suppliers and Registration Authorities. Telia Corporate Security's resources can also be used for internal audits. If any deficiencies turn up in the inspections performed by the Certification Authority, the Certification Authority shall begin the necessary operations to fix them, or shall require their suppliers and Registration Authorities to begin the operations.

2.5.2 The audit performed by an external auditor

The Certification Authority's operations are audited by an external auditor at least annually.

2.5.2.1 The auditor and the required competence

The auditor that the Certification Authority has approved must be a well-known and reputable company in the field, which operates independently of the Certification Authority. The auditor

is required to possess sufficient expertise and knowledge in applying PKI technologies and auditing certification operations.

2.5.2.2 The contents of the audit

The audit assesses whether the Certification Authority operates according to the Certificate Policy and Certification Practice Statement, and whether it complies with its own information security policy. The audit shall review all the certification operation processes, the systems used by the Certification Authority, and their organisation. The audit also includes the Certification Authority's subcontractors and the operations of the Registration Authorities. The external audit is performed regularly, as well as each time that considerable changes are made to the processes and systems.

2.5.2.3 Operations after a deficiency is noted

The auditor sends a report on the results of the audit to the Certification Authority. If there are deficiencies in operations, the Certification Authority shall take measures to fix them.

A plan shall be made to fix the deficiencies noted in the Certification Authority's own operations, and its repair schedules shall be formed on the basis of the seriousness of the deficiency and the time required by the repair procedure.

If deficiencies have been noted in the operations of a Certification Authority's subcontractors, the parties in question are informed of this and the subcontractor is required to fix the deficiencies in a reasonable time.

If the audit leads to any need to change the Certification Practice Statement, this is announced in accordance with the methods described in the document's Chapter 8, "Managing the Certificate Policy"

2.5.2.4 Communicating the results

The auditor's report is intended for the Certification Authority's internal use. The Certification Authority can inform their subcontractors of the results of an audit concerning their own operations. The report may be communicated to third parties, or may be published partially or entirely as decided by the Certification Authority's organisation.

2.6 The confidentiality and publicity of information

The certification system's information is confidential, except when based on the regulations concerning the relinquishment of data in the Personal Data Act or the Act on Strong Electronic Identification and Electronic Signatures, or what has been defined as Certificate Policy, within statutory limits.

The data relinquished to the authorities is defined in accordance with the current legislation. The information in the certification system is not relinquished for any other purpose.

3 The identification of the Certification Authority and the certificate applicant

3.1 The Certification Authority's naming practice Teliasonera Mobile ID CA v1

The Certification Authority has an unambiguous distinguished name (DN) in accordance with X.501, which can be found in the Certification Authority's certificate's Subject field and in the

Issuer fields of all the certificates granted by the Certification Authority. The Certification Authority's name consists of the following attributes:

Attribute	Content
commonName (CN)	Teliasonera Mobile ID CA v1
Organization (O)	Teliasonera Finland Oyj
Country (C)	FI

3.2 The Certification Authority's naming practice Teliasonera Mobile ID CA v2

The Certification Authority has an unambiguous distinguished name (DN) in accordance with X.501, which can be found in the Certification Authority's certificate's Subject field and in the Issuer fields of all the certificates granted by the Certification Authority. The Certification Authority's name consists of the following attributes:

Attribute	Content
commonName (CN)	Teliasonera Mobile ID CA v2
Organization (O)	Teliasonera Finland Oyj
Country (C)	FI

3.3 Naming the certificate applicant

The distinguished name in the Subject field is used as the unambiguous name of the certificate applicant, always containing the following attributes:

Attribute	Content
commonName (CN)	The certificate applicant's name, as follows: Last name First names FINUID or First names Last name FINUID
givenName (GN)	The first names of the certificate applicant
surName (SN)	The last name of the certificate applicant
serialNumber (SN)	An electronic user ID (FINUID)

The technical services (OCSP, time-stamping) may use a different DN value, which includes just the CN value.

3.3.1 Name meanings and interpretation

The commonName attribute contains the certificate applicant's first names and last name. The attribute defines the certificate applicant's registered name, which is saved in the Population Information System of the Population Register Centre. Nicknames and pseudonyms are not used.
Additionally, the attribute contains the Certificate Applicant's electronic user ID (FINUID), which is a dataset formed from numbers and a control digit, and which is used to identify Finnish citizens and foreigners who are living permanently in Finland and have been entered in the Population Information System, as set in the Municipality of Residence Act.

3.3.2 Unambiguity of names

The Subject field in the certificate must be unambiguous to all the user IDs created by the Certification Authority, and must follow the X.500 standard for unambiguity. Unambiguity means that the Certification Authority does not grant different persons certificates with identical field values. The Certification Authority can, however, simultaneously grant the same person several certificates with the same Subject field value.

3.4 Renewing a key pair after revocation

Renewing a key pair always creates a new certificate with new keys. The old certificate and key pair remain closed, and the new certificate is obtained in the same way as obtaining a certificate for the first time.

4 Functional requirements

4.1 Applying for a certificate

A mobile certificate can be granted to a Finnish citizen or a foreigner permanently living in Finland, as set in the Municipality of Residence Act (201/1994), if their personal data has been saved in the Population Register Centre's Population Information System.

The certificate applicant may apply for a mobile certificate at their SIM card issuer's local customer service points or self-service portal.

Applying for a certificate at a local customer service point	The use of a mobile certificate requires a SIM card supporting this feature. If the certificate applicant does not own such a SIM card already, a new SIM card is delivered together with the Mobile Certificate Service order. The Mobile Certificate Service can be ordered and the SIM card replaced in advance of, or at the same time as, applying for a certificate, in accordance with Chapter 4.2.1, "Delivering a tool of identification". The subscription user must personally apply for the Mobile Certificate Service and the related mobile certificate at the SIM card issuer's local customer service point. If the subscription user differs from the subscription orderer, and the subscription orderer has not previously ordered a Mobile Certificate Service for their subscription, the subscription orderer must be personally present when applying for the certificate. The person responsible for registrations at the local customer service point searches for subscription information in the SIM card issuer's system and identifies the subscription orderer in accordance with Chapter 4.2 "Recognising the Certificate Applicant". Before the certificate is granted, the person responsible for registrations gives the certificate applicant the conditions for the Mobile Certificate Service, describing the rights and the duties of both parties. The certificate applicant must approve the conditions related to using the certificate and must validate the correctness of the personal information

Applying for a certificate at a self-service portal	The use of a mobile certificate requires a SIM card supporting this feature. If the certificate applicant does not have such a card in advance, the Mobile Certificate Service and the SIM card must be ordered before applying for the certificate, in accordance with Chapter 4.2.1, “Delivering a tool of identification”. The certificate applicant login into a self-service portal and begins the certificate registration process. The Certification Authority's registration system identifies the applicant using strong electronic identification, in accordance with Chapter 4.2 “Identifying the Certificate Applicant”. Before granting the certificate, the applicant must approve the conditions related to using the certificate and must validate the correctness of their personal information in the system

4.2 Identifying the certificate applicant

A precondition for obtaining the mobile certificate is that the customer has a Finnish personal identity code. The customer’s identity must be reliably identifiable, and it must be possible to connect their personal identity code to it reliably. The mobile certificate applicant is either recognised personally at a Registration Authority’s customer service point or by using strong electronic identification.

Applying for a certificate at a local customer service point	The registration authority will personally verify the applicant’s identity during registration using a valid document that has been granted by a Finnish authority and that proves the person’s identity reliably. Such documents include: - A valid Finnish passport or an ID card granted by the Finnish police - If the certificate applicant’s identity cannot be verified reliably, the applicant’s identity shall be verified by the police. A verification by the police will be charged in accordance with the police’s price list.
Applying for a certificate in the self-service portal	The identity of the certificate applicant is verified during registration on the SIM card issuer’s self-service portal, or by using strong electronic identification provided by a party that has made a statutory announcement to the Finnish Communications Regulatory Authority, and that has made an agreement with the Certification Authority to trust the initial verification of the certification service provider. The supported strong identification services are found at: www.Telia.fi/Teliaid/tunnistusmemetelmatverkkopalvelussa

4.2.1 Delivering a tool of identification

A tool of identification is formed by a SIM card with private keys and the related PINs. The use of the mobile certificate requires a SIM card that supports this function, and the applicant cannot apply for a certificate until they have a SIM card. Only the subscription orderer may order a Mobile Certificate Service and the required SIM card, which is delivered to the subscription orderer personally at a customer service point or by mail, for the subscriptions that they own.

The SIM card is delivered to the customer without a registered certificate.

Ordering a Mobile Certificate Service at a local customer service point	The SIM card is given personally to the subscription orderer when a Mobile Certificate Service is ordered, at the SIM card issuer's local customer service point. This can happen either during the same visit as the registration of the certificate or before it. The PIN of the private keys is created during the registration process to a value set by the orderer.
Ordering a Mobile Certificate Service at a self-service por tal	The subscription orderer can order a Mobile Certificate Service for their own subscription, or for other subscriptions they own, in the self-service portal. The subscription orderer defines the subscriptions and the users for whom the Mobile Certificate Service is ordered. The SIM card is delivered to an address defined by the subscription orderer by mail.

4.3 Granting the certificate

The Certification Authority issues the mobile certificate when it approves the Certificate Application.
The Certificate Application may be approved when the certificate applicant has a SIM card supporting the mobile certificate, the certificate applicant is identified successfully, they have approved the certificate's conditions of use, and they have been registered in the Population Register Centre's Population Information System.

When the applicant applies for a certificate from a local customer service point, the Certificate Application is approved and digitally signed by a local registration authority. At a self-service portal, the approval is performed by the Certification Authority's registration system which sign the certificate request on behalf of the applicant after successful identification of the applicant.

When granting a mobile certificate, the Certification Authority is responsible for its data contents matching the data stated in the application at the moment of issuance.

4.4 Creating a certificate

The Certification Authority's certification system only approves a Certificate Request in the registration system when it can recognise its origin on the basis of the registration system's certificate. The certification system creates a mobile certificate and signs it using the Certification Authority's private key.

The certificate applicant's information for the certificate is obtained from the Population Register Centre's Population Information System, on the basis of the applicant's personal identity code. If the applicant has not previously had an active electronic transaction ID (FINUID), the Population Register Centre activates it during registration and publishes it in its own directory.

During the enrolment process the applicant starts the key generation on the SIM card, select PIN code that protects the keys and proves that he/she possesses the phone that includes the key pair by signing a random nonce using the private key (Proof-Of-Possession). The certificate applicant shall be informed of the granted certificate by mobile phone, and the certificate is published in the Certification Authority's private directory of certificates.

4.5 The end of the certificate's validity period and certificate revocation

4.5.1 The preconditions for closing the certificate

The mobile certificate must be revoked under the following conditions:

- The certificate owner requests the revocation of the certificate (for any reason)
- The certificate owner's private key has or is suspected to have disappeared, been stolen, or been revealed
- The subscription matching the Mobile Certificate is closed
- The certificate owner uses their private key in contradiction to its purpose of use
- The certificate has not been granted in accordance with the proper Certificate Policy or this Certification Practice Statement
- A mistake exists in the certificate information
- The certificate owner or the subscription orderer substantially breaks the agreement made with the Certification Authority
- The certificate owner dies

The certificate may also be revoked in the following circumstances

- The certificate owner or the subscription orderer breaks the agreement made with the Certification Authority
- There is some other particular reason for cancelling the certificate, such as the development of cryptographic attack methods.

Instead of permanently revoking the mobile certificate, a mobile subscription can, upon request, be closed until further notice, if the certificate's owner has lost control of the SIM card but there is no reason to suspect that private key information or activation information has been revealed (such as when a mobile phone has disappeared but its discovery is considered probable). When a mobile subscription is temporarily closed, the use of the private keys saved on the SIM card is prevented.

The revocation request must be made immediately after a suspicion of the possibility of malpractice has been raised.

4.5.2 The party performing the revocation request

The revocation request of a mobile certificate is primarily performed by the owner of the certificate. If the requesting party differs from the owner of the revoked certificate, the requesting party is identified in addition to the owner. The revocation request can also be performed by a Certification Authority, the issuer of the card, or an official authority.

The owner of the subscription can request the revocation of the subscription they own. When a subscription is closed, the related certificates are revoked automatically.

4.5.3 The revocation event

The mobile certificate may be revoked by calling a Revocation Service number. The Revocation Service's contact information can be found in the chapter "Contact information" at the beginning of this Certification Practice Statement. The Revocation Service number takes revocation requests 24 hours a day, 7 days a week.

The Revocation Service can identify the party making the revocation request by requesting the defined information and comparing it to the certificate owner's information, as saved during registration or other operations.

The Revocation Service will revoke the certificate immediately upon receiving the request, identifying the requesting party and noting the request to be valid.

The owner of the subscription may terminate the subscription or Mobile Certificate Service by contacting customer services or visiting a local customer service point. Additionally, a subscription may be terminated at a self-service portal. The subscription's owner is identified at customer services, just as when revoking the certificate. At a self-service portal, the owner of the subscription is identified using a password, and at a local customer service point using an ID card. The SIM card issuer's system sends an automatic certificate revocation request to the Certification Authority's system when the subscription has been closed.

In situations where there is a recognised risk of misuse of the private key, or if it is obvious there is no right to use the key, it may be necessary to revoke the certificate or temporarily close the subscription due to a request by some party other than the aforementioned parties. In these cases, assessing the correctness of the revocation request may require other means of identification. In cases where reliable identification cannot be performed immediately, the Certification Authority may nevertheless decide to revoke the certificate to reduce risks.

The Certificate Authority may also initialise the revocation on the basis of reliable, valid information shown by any party in reference to the revocation conditions in Chapter 4.5.1, "The preconditions for revoking the certificate". As an example, the Certification Authority always revokes the certificates when it has been informed of the death of the owner of the certificate. In these cases, the Certification Authority also announces the termination to the heirs of the deceased certificate owner.

4.5.4 The timing of the revocation event

The revocation of the mobile certificate is performed immediately when processing a revocation request.

4.5.5 Revoking the certificate temporarily

The mobile certificate is always closed permanently, but a mobile subscription may, upon request, be closed until further notice, preventing the use of the private keys saved on the SIM card.

4.5.6 The party performing the temporary revocation request

A temporary revocation of a mobile subscription may be requested by the subscription orderer or user.

4.5.7 The method of performing the temporary revocation request

Requests to revoke mobile subscriptions until further notice are received at the SIM card issuer's customer service unit. The mobile phone is temporarily closed immediately upon receipt of the request, the identification of the requesting party, and validation of the request. The party performing the temporary mobile subscription closure request is identified similarly to when revoking the certificate.

The Certification Authority may also revoke the certificate if it finds that the conditions require this.

4.5.8 Time limits of a temporary revocation

A temporary revocation of a mobile subscription is valid until its cancellation.

4.5.9 Ending a temporary revocation

The request to return a temporarily revoked mobile subscription into use is received by phone at the SIM card issuer's customer service. The request may only be approved if it is from the person who sent the original request for a temporary revocation of the subscription. The basis for approving the request is the password that has been agreed with the customer and saved when closing the subscription.

The name of the person requesting that the mobile subscription is returned to use, the used password, and the time when the subscription is returned to use, are saved.

4.5.10 The frequency of publication of the Certificate Revocation List

The Certificate Revocation List service is implemented by publishing the Certificate Revocation Lists, signed electronically by the Certification Authority, in a public directory. The following rules are obeyed:

- The new Certificate Revocation List is always published in the directory immediately after the approval of the revocation request, or at least at one (1) hour's interval.
- Each Certificate Revocation List is valid for twenty-four (24) hours.

At any given time there may exist several valid Certificate Revocation Lists. The list published most recently contains the most up-to-date information.

During system updates and other exceptional situations, the Certification Authority may publish Certificate Revocation Lists with different frequencies of publication and extended periods of validity.

4.5.11 The Certificate Revocation List's distribution locations

The Certificate Revocation List is published in locations included as a reference in the certificate's field "CRL distribution points". The Certificate Revocation List's addresses have been listed in Chapter 2.1.1

The Certificate Revocation List is available from the directory 24 hours a day, 7 days a week. The Certification Authority is not responsible for any user-experienced service availability, when the fault or interruption is due to systems or services that do not depend on the Certification Authority.

4.5.12 Checking the certificate's status using online access

The Certification Authority uses the OCSP service. The service is available 24 hours a day, 7 days a week. The Certification Authority is not responsible for any user-experienced service availability, when the fault or interruption is due to systems or services that do not depend on the Certification Authority.

4.6 Renewing a certificate

If a certificate has not expired and is not on the Certificate Revocation List, the certificate owner may renew the certificate at a self-service portal by using an existing mobile certificate for identification. New key pairs are generated on the SIM card when renewing the certificate.

If the certificate has expired, the certificate has been closed, the owner of the certificate has lost their private key's PIN, or there is a need to renew the initial identification, the renewal of the certificate mainly happens just like when first applying for a certificate. The difference is that there is no need to replace the SIM card.

The old, valid certificate is revoked automatically when the certificate is renewed.

4.7 System monitoring

4.7.1 Saved information

The Certification Authority saves the following certification-operation-related essential information automatically or manually:

The information related to the life-cycle of the Certification Authority's key

- the creation of the key, its backup copies, and its restore and destruction
- the maintenance events related to the HSM device

The maintenance events related to the life-cycle of the Certification Authority's certificates and the certificate owners

- Certificate Applications and requests, certificate renewal requests for new keys and keys already in use
- certificate revocation events
- certificate creation events
- creation events of the Certificate Revocation Lists

Events connected to maintaining data security

- The changes performed by the Certification Authority's personnel on the certification system and security support systems, including the installations of software, devices, and updates; system shut-downs and restarts; and changes to the system settings

- system outages, hardware faults, and other deviations in systems -
  Events in the routers, firewalls, and intrusion detection systems -
  Events related to access to premises of the certification system.

The saved information includes the information type, date and time, and, in the automatically saved logs, a sequential number and an identifier of the system that produces the log.

At the registration point, the following information is saved:

- Data on the applicant's initial identification and the used identification document -
  The Mobile Certificate Service Agreement made with the certificate applicant
  The following information related to revocation requests is saved at the Certificate Revocation Service
- information on the person asking for revocation
- the date and time when the request was received
- information of the certificate that the user wishes to cancel.

Related to the use of the Mobile Certificate, the following are saved:

- data on the possible blocks and limits of use related to the tool of identification
- data needed for verifying an individual identification transaction and the electronic signature transaction

4.7.2 Monitoring the log information

Important logs related to security and operations are monitored regularly by the Certification Authority's personnel.

To discover suspicious or deviating events, the logs are reviewed based on the alarms created by the systems.

4.7.3 Log data storage period

The certification system's log information is maintained for at a year after its creation. The storage period of other log information created by the Certification Authority's systems varies, depending on how critical the system and the log are, the number of log transactions, and the legal requirements.

Log information may also be moved to a separate log server for archival, and the central information is archived for the period mentioned in Chapter 4.8.2 "Archive storage time". Depending on the system, the log information is delivered as is or in a processed format to another storage medium for archiving.

4.7.4 Protecting the log information

The manually saved logs, and the logs automatically produced by the Certification Authority, are protected from changes, destruction, and illegal access by using the system's access rights management and access control.

The log information of the CA system is protected with a digital signature.

4.7.5 Ensuring the log data

The log data of the certification system is backed up regularly, according to separately defined schedules.

The log information, produced by other than certification system, depends on the system and the criticality of the log information. Backup copies are saved regularly for the most essential log information.

4.7.6 Log data collection system

The Certification Authority's systems support the collection of log data. Certain maintenance events in the production system, such as system changes and updates, and management events related to the Certification Authority's keys, are entered in a different log by hand.

The log information automatically created in the Certification Authority's systems is saved at application level, network device level, and interface level. Manual logs are produced as diaries, in a physical or electronic format, by the Certification Authority's personnel.

4.7.7 System vulnerability testing

The Certification Authority regularly tests the vulnerability of its critical systems, to protect them from external entry attempts. The configurations of firewalls and other systems are updated on the basis of the test results and operation policies and practices.

4.8 Archiving the data related to certificates

4.8.1 Saved materials

The Certification Authority archives at least the following data:

1) data needed for verifying an individual identification transaction and the electronic signature transaction
2) necessary data on the applicant’s initial identification and the used document
3) data on the possible blocks and limits of use related to the tool of identification
4) the certificate’s data contents
5) the Mobile Certificate Service agreement, made with the certificate applicant
6) the logs produced by the certificate system and the manually created logs on tasks related to the certificate system
7) the certificate revocation requests received by the Revocation Service,
8) all published Certificate Policy versions,
9) all the Certification Practice Statements published by the Certificate Authority,
10) reports of external audits.

The data may be archived both electronically and as physical documents.

4.8.2 The storage period of the archives

The information needed to verify an individual identification event and electronic signature event (Chapter 4.8.1, section 1) is maintained for five years after the identification event, and the information on sections 2 - 4 is maintained for five years after the end of the customer relationship between the Certification Authority and the owner of the certificate. Other above-mentioned archived information is maintained for at least 5 years.

4.8.3 Archive protection

The archives containing certification-system-produced data related to the certificate creation and revocation, as well as the certificates themselves, are located in fireproof spaces with

access monitoring, and are also protected with electronic signatures. The same spaces are also used to archive the system's change information and the archives containing the service events.

The archived information produced by the Certification Authority's other systems is archived in spaces protected with access monitoring, either in a locked cabinet or a safe, depending on how critical the stored information is.

4.8.4 Archive certification methods

The electronic archive information produced by the certification systems has backup copies in the case of information loss or destruction, so that if the archive, as such, is destroyed, the information can be returned from backup copies. Backup copies are stored in a physically separate space from the original files.

4.8.5 The acquisition and certification methods of the archived information

Archive information is maintained in a way that ensures that only the Certification Authority's authorised persons can access it. The persons performing an audit in accordance with Chapter 2.2, "Auditing", are authorised to view the archive information. Otherwise, information is only delivered on the basis of a written request, according to the limits allowed and required by the Finnish law, and monitored by Telia Corporate Security.

Archive information shall be relinquished to the certificate owner when it affects them. The information is relinquished without any charges, if it takes place within the limits of the right of verification defined in the Personal Information Act. Otherwise, a payment based on a reasonable amount of work is charged for obtaining information and delivering it.

The Certification Authority ensures that the information needed from its archive at any moment can be obtained and read for the entire period the archive is maintained. This applies to the information in Chapter 4.8.1, sections 1 – 4, even when the Certification Authority's operations are interrupted or come to an end.

4.9 Renewing the Certification Authority's keys

The Certification Authority has a new signature key created before the time of use of the used (old) signature key certificates expires. The Certification Authority also has a new name created for a new signature key, which is shown in the "Issuer" field of the certificates granted by the Certification Authority.

The key is used for signing certificates at most until the last-granted certificate's validity period ends, before the end of the key's period of use. This confirms that the Certificate Revocation List can always be signed using the same key that has been used to sign the certificates on the list.

Together with the replacement of the mobile Certification Authority's keys, the following operations are performed:

a. a new key pair is created for the Certification Authority
b. the Root CA creates a new certificate for the new public key of the Certification Authority and signs it using a private key
c. the new certificate, created in part b), is published in the Certification Authority's directories
d. the new mobile certificates are signed using the new Certification Authority's new private key
e. the old Certification Authority's private key is used for signing Certificate Revocation Lists, until the validity period of the certificate that was last granted with it has ended

The operations performed in connection with the root key's key changes are described in the Root CA Certification Practice Statement.

4.10 Operational continuity management and the processing of exceptional cases

To ensure the continuity of operations in the case of a device fault, the production system has been duplicated to allow the production to move to a back-up device. In such a case, the software is reinstalled. If the data has been corrupted, it is restored from a back-up copy.
A back-up copy of the most critical data is saved at least 4 times a week.
In exceptional and hazardous cases, the Certification Authority follows the process defined in the continuity plan and any other possible directions for this sort of situation, with the aim of minimising the damage caused by exceptional and hazardous cases and ensuring a sufficiently fast recovery.

4.10.1 The Certification Authority's private key has been exposed, or the Certification Authority's certificate has been revoked

If the Certification Authority's private key is exposed, the procedure set by the Certification Authority shall be followed. All the valid certificates granted using the exposed key are revoked using one or several Certificate Revocation Lists whose validity period does not end before the validity period of the last-revoked certificate has ended. After this, the use of the key is ended immediately. When necessary, at the earliest opportunity, the Certificate Revocation Lists signed with this key may be removed from the Certificate Revocation List service, which removes the sufficient basis for trusting the lists signed with the key in question.

If the private key used in the creation of the Certification Authority's certificates, or any other technical method, has been exposed or has otherwise become unusable, the Certification Authority shall announce that the key has been exposed and shall communicate the operations this requires to the certificate owners, service providers, Finnish Communications Regulatory Authority, and other Mobile Certification Authorities. The continuation of operations for the certificate class in question requires the creation of new signature keys for the Certification Authority and the creation of new certificates for the certificate owners.

4.10.2 Endangerment of security due to a natural disaster or some other Catastrophe

The Certification Authority's production locations have been built for safety, taking the probable risks caused by their geographical location into account. In order to minimise the system's vulnerability to failures at any one location, the Certification Authority's most important systems, including the directory services and the Certificate Revocation List's distribution, have been divided geographically into several different locations.

4.11 The termination of the Certification Authority's operations

If the Certification Authority's operations are terminated, the services related to the granting of the certificates are also terminated permanently. The replacement of the Certification Authority's signature keys, or the transfer of the certification operations to another organisation along with the related liabilities, is not seen as a termination of the Certification Authority's operations.

The Certification Authority shall ensure that the certificate owners and the Relying Parties experience as little trouble from the termination of the Certification Authority's operations as possible.

The Certification Authority shall inform their customers and the other Certification Authorities of their identity federation of the termination of their operations as soon as possible, but at least six months before the time of termination.

At least the following processes must take place before the Certification Authority ends their operations:

- All the valid certificates granted using the terminated key are revoked with one or several Certificate Revocation Lists. The validity period of the lists does not end before the validity period of the last revoked certificate has ended.
- The Certification Authority terminates all the authorities they have granted to their contracting partners to perform tasks related to the certificate-granting process for the Certification Authority.
- The Certification Authority destroys or removes their private signature keys from use in a way that ensures they can no longer be used.
- The Certification Authority ensures that the availability of the Certification Authority's archives, mentioned in section 4.8, is maintained even after the Certification Authority's termination.
- The Certification Authority ensures that data is archived as described in the Act on Electronic Signatures, and also that it otherwise generally complies with the regulations of the Archives Act.
- The Certification Authority informs all the subscribers and other Certification Authorities with whom they have made an agreement.
- The Certification Authority ends all the authorisations related to the operations outsourced by the Certification Authority and connected to the certificate authorisation process.
- The Certification Authority ensures that the certificates they have granted can no longer be used or that a sufficient basis no longer exists for trusting them.

5 Physical and operational security requirements and the requirements related to the safety of personnel

5.1 Physical security

The monitoring of physical security is used to control access to the Certification Authority's software and devices. This includes the certification system's servers and workstations, as well as separate encryption-technology devices and encryption-technology tools. An access-monitoring system logs each person entering or leaving the Certification Authority's spaces.

The Certification Authority's private keys, used to sign the certificates and protect the Certificate Revocation Lists, are protected physically in a way that ensures they cannot be revealed as a result of a physical attack.

The back-up copies and data tools have been stored in the Certification Authority's spaces to prevent the loss, tampering with, and unlicensed use of the stored information with sufficient certainty. The back-up copies are stored both for data restoration and archiving of important information.

To implement the principles of physical security described in the data security policy, the Certification Authority shall maintain descriptions of the physical security management of the production system. The most important security principles are documented in a separate

document called “Teliasonera Production CPS”. It can be found from a public repository of the CA at http://repository.trust.teliasonera.com/CPS.

5.1.1 The location and the features of the buildings

The Certification Authority’s secure equipment is located in Finland, in a location whose physical protection is at least equivalent to the requirements set for device spaces of the highest priority class (priority class 1) in the Finnish Communication Regulatory Authority’s Regulation on Securing Communications Networks and Service (FICORA 54/2008 M) .

5.1.2 Physical access to the location of operations

The certificate production locations are guarded and monitored around the clock. Access to the space where the certification system is located has been restricted to certain persons operating in the Certification Authority’s trusted roles. Access to the devices where the Certification Authority’s signature keys are located and where their use is possible requires the presence of two persons with separately granted rights to access the area.

Access to other spaces containing the Certification Authority’s systems other than the registration system has been limited to the authorised persons in charge of maintaining the equipment and the spaces.

Access to the spaces is monitored with an access-monitoring system. If a person has not been granted permanent personal access, they can only move in the spaces when accompanied by someone entitled to access them.

5.1.3 Back-up system arrangements

The Certification Authority’s most central systems have been duplicated in two separate secure device spaces, ensuring that should a device fault occur, it is possible to start using a back-up system without endangering the confidentiality, integrity, and usability of the data in the system.

The certification system’s information is backed up regularly, with the copies stored in spaces separated from the Certification Authority’s production spaces. Access to these spaces has been specifically limited to authorised people. The Certification Authority has maintenance agreements for important equipment, to confirm the acquisition and maintenance of spares.

The device spaces have an automatic fire-alarm system. They are equipped with smoke detectors and handheld extinguishers. Some device spaces use the Inergen gas extinguishing system.

The uninterrupted operation of the certification system is also ensured using a non-interrupting electrical power supply system and back-up power equipment. The device spaces contain a ventilation system, and the air temperature and moisture it produces are monitored continuously. The structural solutions are used to prevent exposure to water damage, and the device spaces are monitored with moisture indicators.

5.2 Operative requirements

5.2.1 Division of responsibilities

The personnel participating in certification operations are divided into trusted roles, with the following responsibilities:

- **Security Manager:** bears full responsibility for managing security practices and verifying the logs created by systems.
- **Certification Authority Administrator:** configuring, maintaining, and performing installation orders for the Certification Authority's trusted systems for registration and the creation of certificates; preparing a tool for offering and delivering the signatures and the revocation of the certificates; handling maintenance and installation orders; and handling the management processes of the PKI fault assessments and the Certification Authority's private keys.
- **System Administrator** Daily access monitoring of the Certification Authority's trusted system, taking back-up copies, deploying the reserve system and managing recovery, and performing installations and system-level fault assessments as ordered.
- **Registration Officer:** approval of the tasks related to the creation and distribution of the certificates.
- **Revocation Officer:** approval of the tasks related to the revocation of certificates, and the tasks related to the Certificate Revocation List

The Certification Authority ensures that sufficient personnel have been hired for each task and that individual persons cannot operate in all the roles simultaneously.

5.2.2 The number of persons required for the tasks

The simultaneous participation of several persons is required for certain tasks.
The implementation of the critical operations related to the production of the certificates in the production spaces requires the participation of at least two people. In accordance with the procedures defined by the Certification Authority, the creation of the Certification Authority's private key, its back-up copying, return, and revocation, and the initialisation of the security module of the Certification Authority's private key require the presence of at least two people.

The use of another system requires the presence of one person who is authorised for the task.

5.2.3 Task-based identification

The identification of those operating in the following roles requires a certificate:

Certification Authority Administrator (certification system)
Registration Manager

In the roles listed below, the identification process mainly relies on a user ID and a password. When dealing with the role-related duties requires the use of the Certification Authority's most critical systems, signing in also requires an identification based on a certificate or one-time password for those operating in the roles listed below.

Certification Authority Administrator (registration system)
Security Manager
System Administrator
Revocation Manager

5.3 Personal security

When hiring the Certification Authority's employees, Telia's normal employment methods are applied, including employment checks. The Certification Authority ensures that each person it has hired for certification-related tasks possesses sufficient qualifications and experience to perform their tasks. Subcontractors whose workers operate in the Certification Authority's important roles sign an agreement that requires them to ensure these matters are handled by their own employees.

Telia has defined and maintains extensive corporate-security-related guidelines (policies, standards, operating guides, definitions, and rules), which each employee must recognise and know.

Each employee who belongs to the Certification Authority's own organisation and who has tasks related to the certification operations signs a personal confidentiality agreement. In addition, each certificate manufacturer or other Certification Authority subcontractor whose workers operate in the Certification Authority's trusted roles signs an encryption agreement that is binding on its employees.

5.3.1 Creating a staff background assessment

The persons operating in the following roles will have their background information checked by a third party:

Security Manager
Certification Authority Administrator
System Administrator

In other cases, the Certification Authority shall check their employees' background information according to their own judgment, depending on the employee's role in the Certification Authority's organisation. The Certification Authority signs agreements with their subcontractors to verify the background information of their employees in important roles.

5.3.2 The method for performing the background assessment

All the background verifications of persons hired for the Certification Authority's tasks follow the employment methods defined by Telia, along with the related employment verifications.

Background verification is done using the basic security assessment drawn up by the police for persons operating in the roles mentioned in Chapter 5.3.1.

The verification is renewed when necessary, in accordance with the Certification Authority's judgment and the limits of the law.

5.3.3 Training-related requirements

The Certification Authority's new employees are trained to perform certification tasks in general, to follow the related security requirements, and, in particular, to perform their own tasks. The processed materials include, among other things, the Data Security Policy, the Certificate Policy, and the Certification Practice Statement. When necessary, individualised training tailored to the person's work tasks and role shall be organised.

The Certification Authority shall instruct their subcontractors' employees on the security requirements of certification operations. Otherwise, the subcontractors themselves are responsible for training their employees in accordance with the agreement.

5.3.4 Maintenance of expertise and know-how

When necessary, complimentary training is organised for the Certification Authority's employees, to ensure that the expertise related to the management of the task is always at the level required by the task.

5.3.5 Operations caused by exceptional situations

In exceptional situations, the Certification Authority may temporarily use personnel that are not fully trained to perform their tasks. Their work shall be directed and monitored by the regular staff, with particular care.

If the Certification Authority finds evidence of malpractice, the Certification Authority's employee at fault is immediately moved to other tasks, and all their rights to access systems connected to certification operations are revoked. The further processing of the case follows Telia's practices currently in force.

When a malpractice case involves a subcontractor, it shall be handled using the methods defined in the agreements.

5.3.6 The documents provided for use by the staff

Each of the Certification Authority's employees hired to perform processes related to the certification operations is offered access to operations and documentation related to the Certification Authority's operations. Additionally, the employees are offered directions and other materials specifically related to performing their own tasks. The directions are also available in electronic format when the employees are using their systems and applications.

The Certification Authority provides the subcontractors with their basic documentation, and the subcontractor is responsible for providing this to their employees. Through their applications, the employees of certain subcontractors can access the guidelines maintained by the Certification Authority. The Certification Authority also delivers documentation personally to the subcontractor's employees who work in certain roles. Additionally, the subcontractors are required to provide all other necessary documentation to their employees.

6 Technical security measures

The general technical security measures related to Telia Company CA services are documented in a separate document called "Teliasonera Production CPS". It can be found from a public repository of the CA at http://repository.trust.teliasonera.com/CPS

6.1 Creating, saving, and deploying a key pair

6.1.1 Creating a key pair

6.1.1.1 Certification Authority

The creation of the Certification Authority's key pair happens in accordance with the key creation process defined by the Certification Authority. The key pair is created in the Certification Authority's physically protected location, in a security module, using a certification system (see chapter 6.2 "Protecting the Certification Authority's private keys") The persons participating in the creation of the keys are the persons authorised for this task by the Certification Authority and operating in trusted roles. At least two such persons must be available on site. The operations of the key creation procedure are entered in the minutes, and each person participating in the procedure shall validate the minutes using their signature. The minutes are maintained in accordance with Chapter 4.8, "Archiving the data related to certificates".

6.1.1.2 Certificate owner

Together with the creation or a renewal of a certificate, key pairs are created in a SIM card's security module. Private keys do not lead to copies being created and may not be transferred or copied from a SIM card.

The Certification Authority, the card issuer, and the card manufacturer may not access the certificate owner's private keys.

6.1.2 Relinquishing the SIM card to the applicant

The process for relinquishing the SIM card to the applicant has been described in Chapter 4.2.1, "Delivering a tool of identification"

6.1.3 Delivering the certificate applicant's public key to the Certification Authority

During the registration of a Mobile Certificate, new keys are created inside the SIM card, the identity of the certificate applicant is connected to an ICCID ID, and the registration system sends a certificate request to the certification system. The certificate request contains a public key and other Mobile Certificate data.

6.1.4 The distribution of the Certification Authority's public key

The Certification Authority's certificate contains the Certification Authority's public key. The Certification Authority's certificate is available in the Certification Authority's directory, in accordance with Chapter 2.1.1 "Publishing the Certification Authority's information".

6.1.5 Key lengths

The private key of the Certification Authority, which is used to sign the Mobile Certificate and the Certificate Revocation List, is an RSA key of least 4096 bits. The key used in signing OCSP messages and timestamps is an RSA key of at least 2048 bits, or an ECC key of 256 bits.

In the case of Teliasonera Mobile ID CA v1, the Certification Authority's key for the certificate owner is an RSA key of at least 1024 bits. In the case of Teliasonera Mobile ID CA v2, the key is an ECC key of at least 256 bits.

6.1.6 The keys' purposes of use

The field defining the purpose of use in the certificate's data content, "Key Usage", defines the purpose of use for the keys related to the certificates (such as digital signature or non-repudiation). The use of the keys is limited solely to their purposes of use.
A key meant for non-repudiation must thus only be used for this purpose, and not, for instance, for identification.

The certificate applicant's card shall have separate keys created for an digital signature, meaning non-repudiation and identification. The Mobile Certificate involves two key pairs and,

likewise, two certificates. A key meant for identification can also be used for consent. Its purposes of use may also include encryption. The certificate's information content has been described in more detail in Chapter 7.1, "The technical information of the certificates".

In the Extended Key Usage certificate expansion, it is possible to save "User certificate" and "E-mail certificate" (Client authentication and Secure Email) as the Mobile Certificate's purposes of use, and this is done every time the signatory is Teliasonera Mobile ID CA v2 or some newer institution. In system certificates, together with the creation of the OCSP messages or timestamps, the purpose of use is a specific purpose of use, intended for these operations.

6.2 Protecting the Certification Authority's private keys

The Certification Authority has implemented the protection of their private signature key with a combination of physical protections, specified procedures, access monitoring, and access rights.

6.2.1 The standards affecting the security module

The certification system, which is located in the Certification Authority's secure, physically protected location, includes a security module used to protect the Certification Authority's signature key. The security module complies with at least the FIPS 140-2 level 3 standard.

6.2.2 The personnel participating in the processing of the Certification Authority's private key

Using technological monitoring and defined procedures, the Certification Authority ensures that no person can, by themselves, obtain the means for accessing the environment where the private key is saved, or for using the key in any way. Critical operations related to the signature key, such as the key's creation, confirmation, and return, are always performed by more than one person.

6.2.3 The back-up copy of the private key

An arrangement exists for restoring the Certification Authority's private signature key to cover for the possibility of it being destroyed. The back-up copying of the Certification Authority's private key has been handled in a way that guarantees, in all situations, at least the same security level as required for the maintenance of the private keys used in the certification system.

The Certification Authority's private keys and their back-up copies are stored using strong encryption. The return of the keys requires the use of Activation Data that has been saved in parts in separate secure spaces and whose availability has been distributed to a number of persons in positions of trust. This number is defined by the Certification Authority. The return of the key requires a certain number of these people to participate in the return procedure.

6.2.4 Archiving the private key

The private keys of the Certification Authority or the user are not archived.

6.2.5 Managing the private key in the security module

The Certification Authority's private keys are only used in the Certification Authority's certification system, located in a safe environment. The activation of the Certification

Authority's private key requires at least one person operating in the Certification Authority's trusted role, identified by the certification system using a strong identification mechanism. The key is maintained as active in the certification system until its use is ended due to, for instance, maintenance operations.

The Certification Authority has created instructionss for the security module's life-cycle management method and for implementing the requirements defined in the Certification Practice Statement and the Certificate Policy.

6.3 Protecting the certificate owner's keys

6.3.1 The standards affecting the SIM card

SIM cards are manufactured in a GSMA-SAS certified factory. They are manufactured in accordance with the ISO 7816 standard and the 3GPP standards TS 31.102 and TS 31.111, as well as TS 23.048.

6.3.2 Relinquishing a private key to a trusted party

The certificate owner's private key is not relinquished to any parties other than the applicant. The private key is only created after the card has been delivered to the subscription owner and the owner has activated the key generation process.

6.3.3 The back-up copy of the private key

No copies exist of the certificate owner's mobile-certificate-connected private keys.

6.3.4 Archiving the private key

No archives exist of the certificate owner's mobile-certificate-connected private keys.

6.3.5 Managing the private key on a SIM card

No specific actions are taken to manage the private key. The private key exists solely on a SIM card.

6.4 Other matters related to managing a key pair

6.4.1 Archiving the public key

The Certification Authority archives all the certificates it has granted, which also leads to the archiving of the public key.

6.4.2 The validity period of public and private keys

The Mobile Certificate's validity period is at most five years. The certificate's validity period may be shorter, if the usable key length is not considered such that it would remain secure for a full five-year period.

The certificate may be revoked during its validity period. The certificate revocation event is discussed in more detail in section 4.5, "The end of the certificate's validity period and certificate revocation".

6.5 The PINs for the private keys on the SIM card

6.5.1 The creation and utilisation of the PIN

The use of the SIM card's private keys has been protected using PINs, which are also used as the private key's activation data. The PIN may contain 4 to 8 digits. The card software generates the PIN at the same time as the key pair is generated on the SIM card. The certificate owner may set the PIN as they wish.

6.5.2 Protecting the PIN

The PIN has been protected in a manner that ensures that they cannot be read or copied from the card.

A private key is locked if the connected PIN is mistyped five (5) times in a row. A locked key cannot be returned to use. If the key is locked or the certificate owner forgets thePIN, the certificate owner must create a new key and register a new certificate in accordance with Chapter 4.6, "Renewing a certificate".

6.6 The certificate system's security requirements related to using and accessing the devices

6.6.1 Device safety

Only devices suitable for their purpose of use are used as certification system equipment. Access to the Certification Authority's device platforms and systems has been limited to persons in trusted roles, as described in Chapter 5.2.1, "Division of responsibilities". The users are identified using strong user identification. The device platform's security settings have been increased, in line with the requirements set by Telia and the Certification Authority.

6.7 The certification system's life-cycle management

6.7.1 Monitoring related to the development of the certificate system

The development of the Certification Authority's production system uses two-phase testing. The changes created as a result of the development process are first tested in a separate development system. After a successful testing round, the changes, along with the production system, are applied in a test system that is as identical as possible, and a final approval test is performed before the changes are delivered into production.
All the changes to the system to be delivered into production are documented carefully.

6.7.2 Management of security

The Certification Authority follows the policy defined by Telia Corporate Security in managing data security. Additionally, the Certification Authority follows, in all of their operations, their self-defined Data Security Policy and their Certification Practice Statement. The auditing of the operations has been described in Chapter 2.5, "Audit".

The maintenance of the business continuation plan created by the Certification Authority includes evaluating the business risks and creating models of operation for the possible risks. The reporting of the deviations and noted or suspected security weaknesses takes place according to the methods of operation set by the Certification Authority.

The Certification Authority ensures the data security of the outsourced operations using agreements, and also ensures that the defined policies and practices are followed when using subcontractors.

6.8 The security of the data network

The Certification Authority's system has been separated from the public network using firewalls. The Certification Authority's network has been divided into different security zones, and the traffic between the zones has been limited using access lists, which permit only the data connections required for the operation and maintenance of the systems. All other traffic has been prevented. The most critical parts of the systems cannot be contacted directly from public networks. A host intrusion detection system is also in use. The most central network components have been duplicated to ensure their usability.

Strong identification and encryption are used in the traffic between the parts of the Certification Authority's systems.

The Certification Authority's root certificate is not in the network at all, but is rather stored in a system that has been detached from the network entirely.

6.9 Monitoring the use of the security module

The Certification Authority's private keys are protected with a security module. Access to the security module has been protected using strict physical and logical access control. The safety mechanisms related to the protection of the security module have been described in Chapter 6.2, "Protecting the Certification Authority's private keys".

The Certification Authority shall log the events related to the management and use of the security module and shall monitor the logs in accordance with Chapter 4.7, "System monitoring".

7 Certificate and Certificate Revocation List profiles

7.1 The technical information of the certificates

The certificate's definition of contents, or the certificate profile, defines the fields used in the certificate. The certificate profile of the Mobile Certificates is the profile defined in version 3 of the ITU X.509 standard. The certificate profile also complies with the document RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

7.1.1 Certificate fields and their contents

7.1.1.1 The basic fields of the certificate

Of the basic certificate fields defined in the X.509 standard, the certificates do not use any other fields than those that are mandatory. The basic fields used in the certificates are listed below:

Field	The field's description and content

Version	This field indicates which version of the X.509 standard matches the certificate. The Mobile Certificates match version 3.
Serial number	The Certification Authority creates a different serial number for each certificate. The number indicated in this field is unambiguous for each certificate created in the Certification Authority's system. The software automatically takes care of the serial number's unambiguity.
Signature algorithm	The signature algorithm is the mathematical rule set used by the Certification Authority's software to perform the certificate's signature. Identifiers have been defined for commonly used algorithms. This field is used to announce the identifier of the algorithm used for signing the certificate. The signature cannot be verified when the used algorithm is not known. The algorithm used for signing the Mobile Certificates is sha256RSA.
Issuer	This field indicates the name of the party granting the certificate. The Issuer name for the Certification Authority granting Telia's Mobile Certificates is in Chapter 3.1, "The Certification Authority's naming practice".
Valid from	The Certificate's period of validity is the period of time that the Certification Authority guarantees to maintain the information on the Certificate's status, which indicates whether the Certificate has possibly been cancelled. The "Valid from" field indicates the date and time the certificate becomes valid.
Valid to	The "Valid to" field indicates the date and time when the certificate is no longer valid. The Certificate may be trusted throughout its entire validity period, unless it has been published on a Certificate Revocation List.
Subject	This field specifies which person holds the private key equivalent to the public key in the certificate. This field contains the unambiguous name of the certificate owner. The contents of this field are described in Chapter 3.3, "Naming the certificate applicant"
Public key	This field indicates the algorithm used with the certificate owner's public key. In Mobile Certificates, the algorithm in question is RSA when the Certification Authority is Teliasonera Mobile ID CA v1, and ECC when it is Teliasonera Mobile ID CA v2. The certificate owner's own public key is also given in this field.

7.1.1.2 The additional fields on the certificate

Certificates use the following additional fields, as defined in the X.509 standard. The additional field is defined as being critical when the system utilising the certificate is intended to abandon the Certification Authority unless it recognises the critical additional field.

Field	Criticality	The field's description and content
Key usage	Critical	The purposes of use of the public key containing the certificate are indicated in this field. The Certification Authority is not responsible for the certificates being used in ways contrary to their intended purpose of use. The purposes of use of the public keys of the certificates are listed below. Identification certificate: digitalSignature, keyEncipherment, Signature certificate: nonRepudiation
Extended key usage	Non-critical	The public key's purposes that differ from those in the field "Key Usage" are indicated in this field. The purpose of use indicated in this field may be known generally or defined by the user for a certain purpose. The values "Client authentication" and "Secure email" can be used in this field.
Authority key identifier	Non-critical	The Certification Authority's public key's identifier is given in this field. The identifier may be used to specify the public key that matches the private key used to sign the certificate. The used value is as defined in RFC5280.
Subject key Identifier	Non-critical	The identifier of the owner of the Certification Authority's public key is given in this field. The identifier may be used to find the certificates containing a certain public key. In Mobile Certificates, the formation of the value is as defined in RFC5280..
CRL distribution points	Non-critical	This field indicates the location to obtain the Certificate Revocation List. In Telia's Mobile Certificates, this field contains a URI-type Certificate Revocation List address. The specific addresses of the Certificate Revocation Lists can be found in Chapter 2.1.1, "Publishing the Certification Authority's information".

Authority Information Access	Non-critical	This field indicates the location for obtaining the Certification Authority's certificate. The field contains a URI-type certificate address for the Certification Authority. This field also indicates the URI for performing the OCSP checks related to the Mobile Certificates.
Basic constraints	Critical	This field indicates whether the certificate in a question is the Certification Authority's certificate or not. If this field is in use, the value on the end entity's Mobile Certificates is "false", meaning that it is not the Certification Authority's certificate.
Certificate policies	Critical	This field is used to indicate the Certificate Policy and Certificate Practice Statements that were used to grant the certificate. The Certificate Policy is identified on the basis of the unique Object Identifier (Object Identifier, OID) given to it. The field includes the following information: Policy Identifier = Certificate Policy's OID Policy Qualifier Info Policy Qualifier ID=CPS, Qualifier = Certification Practice Statement's URI Policy Qualifier Info Policy Qualifier ID=User Notice, Notice Text = Certification Authority's information
Subject Alternative Name	Non-critical	This field contains a URI address of the following type: http://Teliaid.Telia.fi/eid/<Subject SerialNumber>, where <Subject SerialNumber>=certificate owner's FINUID

The X.509 standard also permits self-defined additional fields. The Mobile Certificates use the following additional private fields:

Field	**Criticality**	**The field's description and content**

eidSmartCard SerialNumber	Non-critical	The serial number of the certificate owner's SIM card is shown in this field. This serial number is used to connect the certificate owner to the tool of identification they are using. The serial number is the SIM card's ICCID number. The OID identifying the eidSmartCardSerialNumber attribute is 1.2.752.34.2.1
Identification PathLength	Non-critical	The length of the possible chaining path of the initial identification performed when granting of the certificate is saved in this attribute. Its value is zero when
		the identity has been verified personally from written documents. Otherwise, its value indicates the length of the initial identification's identification chain. The OID identifying the IdentificationPathLength attribute is 1.2.246.277.1.5.4.106

7.2 Certificate Revocation List profile

The information contained in the Certificate Revocation List is described below. The Certificate Revocation List indicates which of the certificates whose period of validity has not yet ended have been revoked.

The Certificate Revocation Lists are in accordance with version 2, which is defined in the ITU X.509 standard. They also comply with the document RFC 5280.

7.2.1 The basic fields of the Certificate Revocation List

All the basic Certificate Revocation List fields defined in the X.509 standard, both mandatory and optional, are used in the Certificate Revocation Lists.

The basic fields used in the Certificate Revocation Lists are listed below:

Field	**The field's description and content**
Version	This field indicates which version of the X.509 standard matches the Certificate Revocation List. The Mobile Certificate Service's Certificate Revocation Lists match version 2.
Signature algorithm	The algorithm used for signing the Certificate Revocation Lists is also used for signing the certificates. The algorithm is sha256RSA.

Issuer	This field indicates the name of the Certificate Revocation List's publisher. In the Mobile Certificate Service, the name is always the same as the name of the party granting the certificates on the list (Certification Authority).
This update	The Certificate Revocation List's date and time of publication.
Next update	The latest possible date and time for publication of the next Certificate Revocation List. The next Certificate Revocation List may be published any time after the publication of the previous Certificate Revocation List, but before the publication of the next Certificate Revocation List announced in it. The Certificate Revocation List's frequency of publication has been described in Chapter 4.5.10, "The frequency of publication of the Certificate Revocation List".
Revoked certificates	This field is used to indicate the serial numbers of the revoked certificates and, separately for each revoked certificate, the time when the certificate was revoked and the reason for revocation.

7.2.2 The Certificate Revocation List's additional fields

The following additional fields defined in the X.509 standard are used for the Certificate Revocation Lists:

Field	**The field's description and content**
Authority key identifier	The public key identifier of the Certificate Revocation List's publisher is given in this field. The identifier may be used to identify the public key matching the private key used to sign the Certificate Revocation List.
CRL number	The serial number indicates how many Certificate Revocation Lists the Certification Authority has published before this one, including the current list. The numbering starts at 1 and always increases by increments of one, as subsequent Certificate Revocation Lists are published. The number lets the user deduce whether a certain Certificate Revocation List will replace some other Certificate Revocation List.

There are no private additional fields for the user to define.

7.2.3 The contents of the Certificate Revocation List rows

For each revoked certificate, the Certificate Revocation List indicates the certificate's serial number and the time when the certificate was cancelled. Additionally, for each closed certificate, the Certificate Revocation List enables the publication of the following additional fields, in accordance with the X.509 standard:

Field	**The field's description and content**

Reason Code	This field is used to indicate the reason for the revocation of each revoked certificate. The reason for revocation may be one of the following: KeyCompromise, CACompromise, AffiliationChanged, Superseded, CessationOfOperation.
Invalidity Date	The Invalidity.date field shows the date when it was known or suspected that the private key had been revealed or the certificate had otherwise become useless. The date may be earlier than the date of revocation for the certificate, which shows the date when the Certification Authority revoked the certificate.

8 Managing the certificate practice

8.1 The method for changing the Certificate Practice Statement

Each time something is changed in the Certificate Policy, the effects of the change on the Certification Practice Statement are also evaluated. The Certification Authority's Certificate Policy management team is responsible for starting the evaluation. There may also be other reasons for changing the document, independent of the Certificate Policy.

8.1.1 Sections that may be changed without informing the users and service providers

Corrections related to spelling or appearance may be performed to this document, as well as changes to its contact information, without this being announced to the users or service providers. Additionally, the parts of the Certification Practice Statement that do not, in the Certification Authority's opinion, considerably affect the certificate owners and the Relying Parties may be changed without a separate announcement.

The document may have translations published in different languages without a separate announcement. When the translation and the Finnish text conflict, the Finnish text takes precedence.

8.1.2 The parts that require informing the users and service providers when they are changed

All the parts of the Certification Practice Statement may be changed by informing the users and service providers of the primary future changes at least 15 days before they become valid.

8.2 Publishing and informing

This Certification Practice Statement is available on the Certification Authority's website. The address is provided in Chapter 2.1.1, "Publishing the Certification Authority's information".

All the proposed changes requiring publication are published on the Certification Authority's website, in accordance with the section "The parts that require informing the users and service providers when they are changed", as set in section 8.1.2. Changes affecting the Terms of Agreement shall be announced in writing to the service providers at the address given in the agreement signatory's contact information.

8.3 The Certificate Practice Statement's change and approval method

8.3.1 The party managing the Certificate Practice Statement

This Certification Practice Statement is managed by Telia's Certificate Policy Management Team. The unit's contact information has been provided at the beginning of this Certification Practice Statement.

8.3.2 The method for changing this statement

The Certification Authority's Certificate Policy Management Team shall review and approve all the changes to this Certificate Practice Statement before their publication.

8.4 Version management

The Certification Authority shall archive all the versions of the Certificate Practice Statement they have approved, and these versions shall be available upon request.

Appendix 1: The duties and responsibilities of the Certification Organisation's parties

Parties and duties	Explanations and clarifications
Certification Authority	
Full responsibility for providing the certificate service.	The Certification Authority has made the proper agreements and formed the contractual relationships for providing the services, including outsourcing, subcontracting, and the use of other third parties. The Certification Authority is also responsible for fulfilling the requirements of this policy in cases where some of the Certification Authority's operations have been outsourced to subcontractors.
Obeys the related legislation, the common practices of the Certification Authorities, and the Certification Authority's own practices, in producing the certificate service.	The Certification Authority's operations are regulated by the • Act on Strong Electronic Identification and Electronic Signatures, or the equivalent EU regulation • The Certificate Policy • The Certification Authority's own Certification Practice Statement documents (CPS)
The production of the certificate service in accordance with the Certification Practice Statement.	The Certification Authority is responsible for the Mobile Certificate being usable from the moment of enrolment throughout its entire Mobile Certificate validity period, unless the certificate has been placed on the Certificate Revocation List. The issuer of the SIM card may terminate the subscription contract due to, for instance, unpaid invoices, which will also lead to the Mobile Certificate being revoked. The Certification Authority is responsible for the security of its own certification system.
Maintains and develops the Certificate Policy	The Certificate Authorities will jointly take care of the development and maintenance of the Certificate Policy.

Identifies the certificate applicant reliably and makes an agreement with them.	The process of identifying the certificate applicant follows the Act on Strong Electronic Identification and Electronic Signatures. The agreement with the applicant meets the requirements of the Act on Strong Electronic Identification and Electronic Signatures. The Certification Authority announces the granting or the revocation of the certificate to the applicant or the Registration Authority. The Certification Authority is also responsible for the Mobile Certificate being enrolled to the person identified in the way required by the Mobile Certificate. If the applicant's identification is performed by an agent (Registration Authority), the Certification Authority, in the agreement they have made with the agent, must require them to follow the process set in law.
Ensures there are no errors in the contents of the certificate data.	Verifies the certificate applicant's personal data from the Population Register Centre's Population Information System. When signing the Mobile Certificate with a private key, the Certification Authority ensures it has verified the personal information on the Mobile Certificate in their Certificate Policy and, in accordance with the methods set in the Certification Practice Statement, from the Population Information System. The Certification Authority is only responsible for the information it has saved in the Mobile Certificate.
Takes care of closing the certificates and publishing the Certificate Revocation Lists.	Each Certification Authority is required to publish the certificates and the Certificate Revocation Lists in a way that ensures they are available to all the parties that need them. The Certification Authority is responsible for delivering the correct Mobile Certificate to the Certificate Revocation List and for the certificates showing up in the Certificate Revocation List at the time mentioned in the Certificate Policy.

Follows the current legislation, the Finnish Communications Regulatory Authority's guidelines, a good level of data security, and good methods of processing information when processing the personal information of certificate owners.	Protects personal data from illegal or unlicensed use, through sufficient technical and organisational operations. Protects all the important information and files related to the certification service from loss, destruction, and counterfeiting. The Certification Authority possesses a data security management system that is sufficient for the certificate services it offers. The personal information relinquished by the certificate applicant to the Certification Authority is not relinquished to others without the applicant's approval, a court decision, or other legally mandated requirements, except as part of the Certificate's data contents. Some information may have to be returned later for legal reasons.
The Certification Authority is a legal person, as set in the currently valid legislation.	Act on Strong Electronic Identification and Trust Services (617/2009)
The Certification Authority has taken care of sufficient arrangements for dealing with the liabilities caused by its actions.	Act on Strong Electronic Identification and Trust Services (617/2009)

The Certification Authority is financially stable and has sufficient economic resources to operate as set in this Policy.	Act on Strong Electronic Identification and Trust Services (617/2009)
The Certification Authority has sufficient employees to offer certification services, with sufficient training, technological know-how, and experience, considering the nature, coverage, and volume of the certificate services.	Act on Strong Electronic Identification and Trust Services (617/2009)
The Certificate Authorities that take care of the operations related to creating and cancelling certificates must have a well-documented structure.	Act on Strong Electronic Identification and Trust Services (617/2009).

Registration Authority (RA)	
Takes care of the identification of the certificate applicant on behalf of the Certification Authority, as set in the Certification Practice Statement. The Registration Authority operates on account of and as the liability of the Certification Authority, as set in the agreement between the Certification Authority and the Registration Authority.	Delivers proper and complete certification requests to the Certification Authority when the applicant is applying for a first certificate, renewing a certificate, and renewing key pairs. Identifies the applicant in accordance with this Certification Practice Statement. Ensures that the directions of use for the Mobile Certificate have been delivered to the certificate applicant before the agreement has been signed. The subscription orderer's permit for utilising the paid additional service, insofar as this is necessary. These also apply in cases where the Certification Authority operates as the Registration Authority.
The SIM card issuer	
Ensures the confidentiality of the signature's generation information. Does not save or copy the signature creation generation relinquished to the certificate's owner.	If keys are created on a card, the card issuer is responsible for the security of the platform for running the key generation program, as well as for the key generation application, the reliability of the card's security module, and the confidentiality of the private key.
Certificate owner	

Offers their full and complete personal information to the Certification Authority or its representative when registering, in accordance with this policy.	The Registration Authority is, for its part, responsible that the information given by the certificate applicant is complete and flawless. The certificate applicant validates the personal data with their signature or equivalent.
A name change must be announced to the Certification Authority at most three months after the change.	The agreement between the Certification Authority and the certificate owner must require the user to do this.

Maintains the tool of identification and the related PINs carefully, to prevent the unlicensed use of the Mobile Certificate.	Defined as the duty of the certificate owner in the Act on Strong Electronic Identification and Trust Services (617/2009). The Certification Authority must take this into account in the agreement it has made with the certificate owner. The certificate owner must use PINs to protect their keys and must maintain these PINs carefully. The Mobile Certificate forms their user's electronic identity. Thus, it may not be relinquished to other people. The Mobile Certificate's owner is responsible for using the certificate, for the legal operations they have performed using them, and for the financial consequences caused by their legal operations.
The certificate owner must make an immediate announcement to the Certification Authority's Revocation Service	Defined as the duty of the certificate owner in the Act on Strong Electronic Identification and Electronic Signatures. The Certification Authority must take this into account in the agreement it has made with the certificate owner. The announcement must be made immediately, when: • The certificate owner has a reason to suspect that their SIM card has disappeared, been stolen, or been used in an unlicensed manner; • the certificate owner has lost control of their private key due to the fact that its Activation Data (PIN) has disappeared or fallen into the wrong hands, or for some other reason; • the certificate owner has discovered that the certificate's information no longer applies or that it contains misleading information. The Mobile Certificate's owner's responsibility for using the certificate ends when they have announced that they have given the revocation service sufficient information to revoke it. After this, responsibility is transferred to the Certification Authority. The revocation announcement must be made

	immediately after the reason for the announcement is noted. The certificate owner must maintain their private keys carefully to prevent the unlicensed use of their private keys. In practice, this refers to the related PINs.
The Relying Party of the certificate	
Inspects and verifies the validity of the certificate when using the certificate.	The Relying Party of the certificate must verify the validity of the certificate in the following way: • Verifying the authenticity and the integrity of the certificate by inspecting its granter's electronic signature using the certificate granter's public key. • Obtaining the certificate revocation information from at least one address saved on the certificate. • Verifying the authenticity and the integrity of the certificate by inspecting the electronic signature of the party that has granted it and the validity of the certificate used for the signature. • Verifying the extent of the revocation information period. The certificate shall not be approved unless up-to-date, valid revocation information is available. All the certificate approvals in cases where up-to-date information is missing take place as the risk of the certificate's Relying Party. • It must be confirmed that the used certificate is not closed on the basis of its revocation information. • It must be verified that the granted certificate suits its purpose of use in the legal task for which it has been used.
Saves the information related to the use of the certificate.	The Relying Party is responsible for maintaining the information it needs to confirm the operations performed using the Mobile Certificate at a later time. Such information includes the used certificates and Certificate Revocation Lists, as well as the signature's creation time, which should also be noted in the signed data contents.