Telia Public Key Infrastructure (PKI) Disclosure Statement

Prepared by Telia Certification Authority Policy Management Team

Release: 1.0
Valid From: 2021-05-14
Classification: Public

1. Introduction

The document, the Telia Public Key Infrastructure (PKI) disclosure statement, is for use as a supplemental instrument of disclosure and notice by Telia. It does not replace the existing Certificate Practice Statement (CPS) documents.

2. Definitions

Affiliate	A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Certification Authority (CA)	CA is an entity such as Telia that is authorized to create, sign, distribute, and revoke certificates. CA is also responsible for distributing certificate status information and providing a repository where certificates and certificate status information is stored.
CA/Browser Forum	A group of representatives from certificate authorities and browser vendors to discuss issues surrounding the existing market for server certificates, e.g., certificates used in authenticating TLS-enabled web sites and other servers (e.g., mail servers) to users.
Certificate	An electronic document issued by Telia to a person or entity mainly for verifying the identity of the sender/receiver of an electronic message, and/or for providing the means to encrypt/decrypt messages between sender and receiver (e.g., binding an entity to their public key).
Certificate Request	A process where a natural person (the Subscriber or someone employed by the Subscriber) or an authorized agent with the authority of representing the Subscriber that completes and submits a certificate requestion.
Client Certificate	A digital certificate in which information about the organization and email of holding the certificate has been validated by Telia.
Certificate Practice Statement (CPS)	CPS is a document that defines the legal, commercial and technical practices for approving, issuing, using and managing Telia Server and Client certificates. It also outlines the roles and responsibilities of the parties involved in maintaining the Telia public key infrastructure.
Digital Signature	A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.
Domain name	The label assigned to a node in the Domain Name System.
Domain Validated (DV) TLS Server Certificate	A digital certificate for a web site or other server in which the information about the domain name has been validated by Telia.
Registration Authority (RA)	An employee or agent of an organization unaffiliated with Telia who authorizes issuance of certificates to that organization.
Fully Qualified Domain Name (FQDN)	A domain name that specifies its exact location in the tree hierarchy of the Domain Name System.
OV TLS Server Certificate	A digital certificate in which information about the business entity holding the certificate has been validated by Telia.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Relying Party	Anybody who relies on the certificates issued by Telia (including all end users and operating system vendors who trust Telia certificates).
Repository	An online database containing publicly-disclosed Telia PKI governance documents, and certificate status information, either in the form of a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) response. https://cps.trust.telia.com.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Service Element	The CA internal systems, processes or services such as certificate enrolment, PKI support, backup and system monitoring.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subscriber	A person or entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement and Terms of Use.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the CABF requirements when the Applicant/Subscriber is an Affiliate of the Telia CA or is the CA.

3. Telia CA contact info

- **Email:** cainfo@telia.fi
- **Web**: http://cps.trust.telia.com/
- **Customer Service:** +358 20 693 693
- **Revocation Service Phone:** +358 800 156 677
- **Postal Address:**
  Telia Finland Oyj (1475607-9)
  FI-00510 Helsinki, Finland

4. Certificate type, validation procedures and usage

The following certificate types are issued by Telia:

I. **Telia TLS DV certificate:** to authenticate servers and establishing secure Transport Layer Security (TLS) sessions with end clients. In this type, the domain name the server domain name is validated by Telia.

II. **Telia TLS OV certificate:** to authenticate servers and establishing secure TLS sessions with end clients. In this type, domain name of the server, existence of the organisation and other attributes including name, type, status, and physical address is validated by Telia.

III. **Telia client certificate**: for identifying individual users, securing email communications and document signing.

IV. **Telia document signing:** for authenticating documents from Adobe PDF, Microsoft Office, OpenOffice, and LibreOffice.

Telia provide the above certificate types according to the below certification authorities.

- **TeliaSonera Root CA v1**
  - **Telia Domain Validation CA v2 (I)**
  - **TeliaSonera Server CA v2 (II)**
  - **TeliaSonera Class 1 CA v2 (III)**
  - **TeliaSonera Class 2 CA v2 (III)**
  - **Ericsson NL Individual CA v3 (III)**
  - **TeliaSonera Email CA v4 (III)**

- **Telia Root CA v2**
  - **Telia Domain Validation CA v3 (I)**
  - **Telia Server CA v3 (II)**
  - **Telia Class 3 CA v1 (III)**
  - **Telia Document Signing CA v3 (IV)**

Telia validates the provided information from the subscriber before issuing the certificate to ensure correctness of the certificate contents. Telia publicly trusted certificates are validated against WebTrust or ETSI audits annually.

5. Reliance limits

There is no restriction in using the Telia certificates unless otherwise indicated either in the certificate, in the service description, in applicable CPS text, or in other terms and conditions supplied.

6. Obligations of subscribers

The obligations of the subscribers are listed in the Telia "Subscriber Agreement and Terms of Use "[1]. The current version of the document is published at the Repository.

7. Obligations of relying parties

The obligations of the Rely Parties are listed in the Telia "Relying Party Agreement"[2]. The current version of the document is published at the Repository.

8. Limited warranty and disclaimer/Limitation of liability

Liability for damages and limitations of liability are defined in *Telia´s general delivery terms for business customers concerning services*. In addition to what is mentioned in the aforesaid terms, Telia is not liable for damages arising when the Subscriber does not fulfil his responsibilities as a user of certificates according the requirements defined in the applicable CPS document.

[1] Telia CA Subscriber Agreement and Terms of Use ,
https://support.trust.telia.com/download/CA/Telia_Subscriber_Agreement.pdf
[2] Telia CA Relying Party Agreement,
https://support.trust.telia.com/download/CA/Telia_Relying_Party_Agreement.pdf

9. Applicable agreements, CPS, CP

The applicable documents are published as below at the Telia Repository:
http://cps.trust.telia.com/

1. Subscriber Agreement and Terms of Use
2. Relying Party Agreement
3. Telia Server and Client CP/CPS documents
4. PKI Disclosure Statement (PDS)

10. Privacy policy

Telia does not collect any sensitive or confidential data from Subscriber. Except in scenarios where the CA or RA archive copies of identification documents to validate the identity of a Subscriber. The collected personal information will not be used for any other purpose and Telia's privacy policy[3] governs the CA operations. Telia's Privacy Notice applies to all processing of personal data[4].

11. Refund policy

Telia offers an end of the month period refund policy, where a Subscriber may request a full refund before terminating current calendar month from the day certificate was issued.

12. Applicable law, complaints and dispute resolution

Telia will comply with applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information. In the event of disputes, the parties shall come to an agreement taking into account any applicable laws, regulations, and agreements made. The place of dispute is Telia Finland Oyj, Helsinki, Finland.

13. Telia CA repository licenses, trust marks, and audit

The intellectual property rights of all the software, documents, and other material needed for providing certification services, belong to Telia CA or to a third party. The terms on license to use software and documents, detailed in *Telia´s general delivery terms for business customers* concerning services (available on the internet on Telia web pages), shall apply.

Telia CA services are regularly audited by an independent, qualified third party against WebTrust or ETSI standard EN 319 401 and EN 319 411-1 requirements.

[3] Telia Group Policy - Privacy and Data Protection: https://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/public-policy/group-policy---privacy-and-data-protection.pdf
[4] Telia Privacy Notice: https://www.telia.fi/tietosuoja-ja-tietoturva/privacy-notice