Telia CA

Customer Responsibilities and Subscriber Agreement

Responsibilities of Relaying Party

Responsibilities of Certificate Holder

Responsibilities of Customer Registration Authority

Date: 23rd March 2017

Version: 2.1

Publisher: Telia Finland Oyj

Company information

Telia Finland Oyj

Teollisuuskatu 15, 00510 HELSINKI, FI

Registered office: Helsinki

Business ID 1475607-9, VAT No. FI14756079

OVERVIEW

Certificates issued by Telia CA are utilized in connection with several security services offered by Telia or other parties. This document includes the obligations and responsibilities for the users trusting, using or registrating Telia certificates. The text is divided into these chapters according to the role of a user:

A. Responsibilities of Relaying Party

B. Responsibilities of Subscriber and Holder

C. Responsibilities of Customer Registration Authority

“Relaying party” is anybody who relies on the certificates issued by Telia (including all end users and operating system vendors who trust Telia certificates. “Subscriber” is a natural person or legal entity to whom a certificate is issued and who is legally bound by a Subscriber Agreement text (below). “Holder” (or owner) may be different from Subscriber if a certificate and related keys are given to any third person who doesn’t have direct legal bound with Telia. “Registration Authority” means that a Customer (subscriber) is applying certificates to his users or partners (which are holders).

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT TRUST OR USE TELIA CERTIFICATES.

More detailed terms and conditions can be found from Telia´s general delivery terms for business customers or from applicable Certificate Policy and Certification Practice Statement documents (available on the internet on Telia web pages)

A. RESPONSIBILITIES OF RELAYING PARTY

When utilizing certificates issued by Telia CA, in connection with a service offered by Telia, or otherwise, the user commits to fulfilling the conditions given below.

A.1 Certificate Policy and Certification Practice Statement

The User shall commit himself to fulfilling the procedures described in the applicable Certificate Policy (CP) and in the Certification Practice Statement (CPS). The CP and CPS are available on the internet at https://repository.trust.teliasonera.com. The most important obligations are listed below.

A.2 Relying on a certificate

To be able to reasonably rely on a certificate the user shall at least:

- Verify the authenticity and validity of the certificate using common PKI rules,
- Verify from a valid Certification Revocation List (CRL) or via OCSP that the certificate has not been revoked or suspended,
- Take into account any limitations on the usage of the certificate indicated either in the certificate, in the service description, in CP or CPS text, or in other terms and conditions supplied.

Note. Certain services offered by Telia include verification of the authenticity and validity of the certificate by Telia on behalf of the Customer.

A.3 Certificate usage

The Customer is obliged to use a certificate only for legal and good practice purposes according to the orders and directions of the authorities. The Customer is responsible for the use of the private keys and certificates of the Users related to his organization, for the legal acts the keys and certificates are used for, and for the possible damage caused by this. Telia shall not bear the responsibility of the use of a certificate by the systems utilizing a certificate, or for the contents, legitimacy or enforcement of possible agreements, commitments or other legal acts executed by using a certificate.

The Customer is responsible for the purchase and costs of telecommunication connections needed for utilizing certificates. The Customer is responsible to ensure that the Users follow the applicable terms and conditions, for instruction the Users, for defining the possible restrictions on use of the private keys, for enforcement of the restrictions in their data systems, and for other matters related to the relationship between the User and the Customer.

A.4 Intellectual property rights

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.

A.5 Liability for damages

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 Customer does not fulfill his responsibilities as a user of certificates according the requirements defined in this document.

B. RESPONSIBILITIES OF SUBSCRIBER AND HOLDER

This chapter describes shortly the obligations and warranties for all Telia CA certificate subscribers and holders. This Agreement shall remain in effect until the Certificate has expired or is earlier revoked.

B.1 Responsibilities of relaying parties

All responsibilities listed in the previous chapter (A. Responsibilities of relaying party) shall apply to Certificate subscribers and holders also.

B.2 Accuracy of Information

The subscriber is obliged to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;

B.3 Protection of Private Key

The subscriber is obliged to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token)

B.4 Acceptance of Certificate

The subscriber is obliged to review and verify the Certificate contents for accuracy. If subscriber is separate person from holder, the former has obligation to forward these requirements to certificate holder.

B.5 Use of Certificate

The subscriber is obliged to install the Certificate only on servers or devices that are accessible at the subjectAltName(s) listed in the Certificate or are otherwise applicable, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with these Subscriber Agreement requirements

B.6 Reporting and Revocation

The subscriber is obliged to promptly cease using a Certificate and its associated Private Key, and promptly request Customer's Registration Officer or the CA to revoke the Certificate, in the event that: (a) any essential information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the public Key included in the Certificate

B.7 Termination of Use of Certificate

The subscriber is obliged to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise

B.8 Responsiveness

The subscriber is obliged to respond to the CA's instructions concerning Key Compromise or Certificate misuse within reasonable time period

B.9 Acknowledgment and Acceptance

The subscriber is obliged to acknowledge and accept that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of this document

C. RESPONSIBILITIES OF CUSTOMER REGISTRATION AUTHORITY

The Customer shall assign one or several Registration Officers that are in charge of registration authority duties in the Customer's organization.

C.1 Responsibilities of Certificate subscriber and holder

All responsibilities listed in the previous chapter (B) shall apply to Registration Officers also.

C.2 Registration Officers

A person chosen shall be a reliable and experienced employee of the Customer or of a subcontracting organization serving as a Registration Authority. When subcontracting the registration duties, the Customer is responsible for the operation of the subcontractor as a Registration Authority as for his own.

A Registration Officer has the right to register only such users that belong to Customers own organization or have contractual relationship with the Customer, upon acceptance by the Customer, or such devices that are owned by the Customer. Customer can register only such subject names which are owned by him or Customer has otherwise right to use such names.

The Registration Officers assigned by the Customer shall be bound to familiarize themselves with the Instructions for Registration Officers provided by Telia (e.g. Telia Secure Manager manual) and to act accordingly. Especially a Registration Officer shall take care of the responsibilities listed next in chapter C.3.

C.3 Responsibilities when registering (applies also to renewal and rekey)

Verify the identity of the User (or Device) for certificate application.

Ensure that the User or Device is authorized to apply for a certificate

Verify the authenticity of the information given for the certificate application. Especially verify that common names, domain names, IP addresses and organization names and all other attributes used in certificate subjects are correct and belong to the certificate holder.

Ensure that the commonName representing the user is unique in the Customer's domain.

When the name of the User in the certificate is a pseudonym (e.g. User1), ensure that the pseudonym comprises one single word without any spaces.

When the name of the User in the certificate is represented by a pseudonym, ensure that the genuine identity of the User is known at least throughout the validity period of the certificate.

Submit the certificate request or the information for certificate application to the CA according to the instructions provided.

When the User's key pair has been generated by the Customer or the User himself, ensure that the certificate request is signed by using the private key of the key pair where the public key is the one requested to be certified. Ensure that the key quality is adequate according to CP/CPS.

Use the registration tools supplied by Telia only according to the instructions provided.

Ensure that the private key and the related PIN code are securely delivered to the rightful User and securely stored at all times.

C.4 Cancellation (Revocation)

Certificate revocation is required without unnecessary delays when:

- Upon suspected or known compromise of the private key;
- Upon suspected or known compromise of the media holding the private key;
- Subject or subscriber information is known to be invalid or re-verification fails.
- When there is an essential error in the certificate or

- When any information in the certificate changes;
- Upon termination of a Subject or when a Subject no longer needs certificates;
- When the certificate is redundant (for example, a duplicate certificate has been issued).
- Customer's certificate contract with Telia has ended.
- Any other reason that makes the certificate obsolete or threats related keys

Revocation may be done directly by the Registration Officer or a notification for revocation may be given to Telia's Revocation Center. Access details can be found from CPS documents.

C.5 Authentication of Registration Officers

When the Customer is using an application programming interface (API) or Certificate Application supplied by Telia for User registration, the Customer is responsible for verification of the identity of the Registration Officer using this interface or application. Authentication to registration systems has to be done by a personal certificate or equally strong method every time the API or application is used for registration.

C.6 Security

The Customer shall ensure that he manages securely his part of the certificate registration process. The Registration Officer workstations shall be located in premises secured with physical access control. Each registration Officer shall use his securely stored personal credentials. The Customer shall ensure that unauthorized persons can't use the registration privileges.

C.7 Recording and filing

The Customer is responsible for recording and filing the relevant actions, data and documents associated with the certificate application process, and for storing them for as long as the Customer acts as a Registration Authority and uses certificates issued by Telia CA.

C.8 Chained responsibilities

The entitled Customer's Administrative Contact person shall appoint a Registration Officer for his organization. The Administrative Contact Person is entitled to appoint new Registration Officers and also cancel their rights in the organization as necessary. All Registration Officers have the right, delegated by the Administrative Contact Person, to make the necessary entries and configurations into the data systems to authorize new Registration Officers. The Administrative Contact Person together with old Registration Officers shall ensure that the new Registration Officers will be familiarized with their responsibilities and obligations and instructed in their duties.

C.9 Confidentiality

The terms concerning confidentiality in Telia´s general delivery terms for business customers concerning services shall apply. The Customer shall commit himself to follow the legislation concerning personal data protection in registration.

C.10 Inspection rights

Telia is entitled to verify by inspection that the Customer fulfils the requirements concerning a Registration