Sonera CA

Customer´s Responsibilities

Certificates issued by Sonera CA are utilized in connection with several security services offered by TeliaSonera Finland Oyj ("Sonera"). Certificates may also be used separately with the Customer´s own applications. This document includes the responsibilities and obligations of the Customer as a user of certificates issued by Sonera CA.

The Customer may also act in the role of Registration Authority for applying certificates for his Users. This document includes the responsibilities of the Customer as a Registration Authority as well as the instructions for Registration Officers.

The Customer´s responsibilities, obligations and instructions are divided into the following chapters:

- *A Customer's responsibilities as a user of certificates*
- *B Responsibilities of a Certificate Holder (User)*
- *C Customer's responsibilities as Registration Authority*
- *D Instructions for Registration Officers*

Definitions	
user of certificates	relying party, party that relies on the data in certificates in making decisions
Registration Authority	entity that is responsible for identification and authentication of certificate subjects
User	certificate subject, certificate holder, entity associated with the public key in the certificate

TeliaSonera Finland Oyj
Networking Solutions
Security and Management Services
Kuortaneenkatu 1
P.O. Box 543
00051 SONERA
Finland
Tel: +358 (0) 20401

E-mail: cainfo@sonera.com
Customer Service: 0800 188188 (mon-fri 8-17)
Technical Customer Service (24 h): 0800 180191
Revocation Service: 0800 156677
Internet: http://support.partnergate.sonera.com/Sonera-CA.php

A Customer's responsibilities as a user of certificates

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

1. Certificate Policy and Certification Practice Statement

The Customer shall commit himself to fulfilling the procedures described in the applicable Certificate Policy, CP (Sonera CA Varmennepolitiikka) and in the Certification Practice Statement, CPS (Sonera CA Varmennuskäytäntö) when ordering certificates and when acting as Registration Authority or Relying Party. The CPs and CPS are available on the internet at http://support.partnergate.sonera.com/Sonera-CA.php.

2. Relying on a certificate

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

- Verify the authenticity and validity of the certificate,
- Verify from a valid Certitication Revoction List (CRL) 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 or in other terms and conditions supplied.

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

3. Using certificates

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.

Sonera shall not bear the responsibility of the use of a certificate by the Customer, for the Customer's data systems utilizing a certificate, nor 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.

4. Responsibility for the use of a private key in connection with certificate revocation

The Customer is responsible for requesting revocation of the certificate of a User related to his organization under the conditions described in chapter C item 12). Sonera is not liable for illegal use of the private key of a User related to the Customer's organization, or the damage caused thereby. Sonera is responsible for publishing the revocation status information of a certificate on a Certificate Revocation List (CRL) after reception of the revocation request for the certificate.

5. Intellectual property rights

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

6. Liability for damages

Liability for damages and limitations of liability are defined in *Sonera´s general delivery terms for business customers concerning services*.

In addition to what is mentioned in the aforesaid terms, Sonera 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 a Certificate Holder (User)

The Customer is obliged to ensure that the Users related to his organization are bound to the following responsibilities:

1. The User shall give accurate and complete information with regards to registration.
2. The User shall permit recording of the registration information as well as the certificate itself and the certificate generation and revocation information.
3. The User may use his private key only for purposes allowed by the Customer, and according to the restrictions notified to the Customer.
4. The User shall not give his private key for use by another person.
5. The User shall take adequate precautious to prevent unauthorized use of his private key.
6. The User shall without any reasonable delay submit a notification for delivery to the Revocation Service if any of the following occur up to the end of the validity period indicated in the certificate:
   - the User has reason to believe that his private key has been lost or stolen, or potentially compromised or taken illicitly into use,
   - the User has reason to believe that he has lost control over his private key due to compromise or loss of the activation data (PIN code),
   - the User comes to know that some information in the certificate is inaccurate or should be changed (including e.g. given name, surname, or e-mail address with certain services).
7. Following a compromise of the User's private key or PIN code, the use of the private key is immediately and permanently discontinued.

C Customer's responsibilities as Registration Authority

The Customer shall assign one or several Registration Officers that are in charge of User registration in the Customer's organization. A person chosen as a Registration Officer 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 the Customer's own organization or that have contractual relationship with the Customer, upon acceptance by the Customer.

The Registration Officers assigned by the Customer shall be bound to familiarize themselves with the Instructions for Registration Officers (chapter D in this document) and to act accordingly.

A Registration Officer shall take care of the following responsibilities when registering Users (applies also to certificate renewal and rekey):

1. Verify the identity of the User for certificate application.
2. Ensure that the User is authorized to apply for a certificate.
3. Require the User to provide appropriate information for certificate application.
4. Verify the authenticity of the information given for the certificate application.
5. Ensure that the commonName representing the User's name in the certificate is unique in the Customer's domain.
6. 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, which indicates a pseudonym.
7. When the User's name 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.
8. Submit the certificate request or the information for certificate application to the CA according to the instructions provided.
9. 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.
10. Use the registration tools supplied by Sonera according to the instructions provided.
11. Ensure that the private key and the related PIN code are securely delivered to the rightful User.
12. Submit a notification to Sonera's Revocation Service without any reasonable delay, when:
    - there is reason to believe that the User's private key is no more in his sole possession,
    - the contractual relationship between the User and the Customer is terminated whereupon the certificate is no longer needed for the original purpose,
    - according to the Customer's judgment there is no more reason for the use of the certificate.
13. Require revocation of the User's certificate and submit a new certificate request when it becomes apparent that there is invalid information in the certificate but the prerequisites for the use of a certificate by the User are still valid. This information includes e.g. the User's given name, surname, commonName (CN), and e-mail address with certain services.

When the Customer is using an application programming interface (API) supplied by Sonera for User registration, the Customer is responsible for verification of the identity of the Registration Officer using this interface. This has to be done by a certificate every time the API is used in registration.

The Customer shall ensure that he manages securely his part of the certificate application process. The Registration Officer workstations shall be located in premises secured with physical access control.

The Customer is responsible for recording and filing the 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 Sonera CA

The 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, upon the requirement from the Administrative Contact Person, to make the necessary entries and configurations into the data systems to authorize new Registration Officers. The Administrative Contact Person shall ensure that the new Registration Officers will be familiarized with their responsibilities and obligations and instructed in their duties.

Among of the Registration Officer duties are registration of new Registration Officers for certificate application and submission of a notification to the Revocation Service when the rights of a Registration Officer have been cancelled. The Customer's Administrative Contact Person has the ultimate responsibility for requesting revocation of a Registration Officer's certificate when the Customer wants to cancel the rights of that Registration Officer.

C1 Confidentiality

The terms concerning confidentiality in *Sonera´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.

C2 Inspection rights

Sonera is entitled to verify by inspection that the Customer fulfils the requirements concerning a Registration Authority and that the Customer's Registration Officers follow the registration instructions provided.

C3 Liability for damages

Liability for damages and limitations of liability are defined in *Sonera´s general delivery terms for business customers concerning services*.

In addition to what is mentioned in the aforesaid terms, Sonera is not liable for damages arising when the Customer does not fulfill his responsibilities in registration according the requirements defined in this document.

D Instructions for Registration Officers

These instructions are intended for use in the organizations of Sonera's Customers that act in the role of Registration Authority. The Customer shall appoint one or several Registration Officers that have the right to register Users in the organization for certificate application. Every Registration Officer shall familiarize himself with these instructions and perform his duties accordingly.

Instructions for the software tools used by Registration Officers will be delivered separately.

1. Registration Officer certificate

The Customer's Administrative Contact Person named in the contract between Sonera and the Customer shall appoint one or more Registration Officers and order him/them certificates using a subscription form. Sonera will deliver to the Registration Officer one of the following:

1) certificate on a smart card and a PIN code,
2) certificate on a USB token and a PIN code,
3) one time password and instructions for a software certificate request.

The Customer's Registration Officer has the right, upon the requirement from the Administrative Contact Person, to define new Registration Officers into the system and order/apply certificates to them.

A Registration Officer shall keep his smart card or USB token safe so that nobody else is able to use it. The PIN code may not be kept so as to be seen or to be associated with the smart card or USB token in any circumstances. If the Registration Officer uses a software certificate he shall protect his workstation and keep his PIN code only to himself. A Registration Officer is in person responsible for any operations made using the private key associated with the certificate issued to him.

When the Customer is using an application programming interface (API) supplied by Sonera for User registration, the Registration Officer shall always use certificate-based authentication into the system when he uses the API.

2. Registration of Users

A Registration Officer is entitled to register only Users that belong to his own organization or have contractual relationships with his organization. The Users shall have authorization from the Customer's Administrative Contact Person to apply for a certificate.

It is essential that a certificate will be issued to the authenticated User. The Registration Officer shall ensure that the name information included in the certificate is correct. The certificate application process shall be discontinued if a mistake occurs in the certificate application information. If a mistake is detected afterwards the certificate containing incorrect information shall be revoked and a new certificate request with correct information shall be submitted.

Information recorded earlier about a User by his company or organization may be used for User identification. When this is not appropriate the User applying for a certificate shall prove his identity by presenting an identity card.

If the User's name in the certificate is a pseudonym the Registration Officer shall maintain information of the genuine identity of the User. The User's identity shall be available when necessary during the whole validity period of the certificate.

3. Delivery of certificate, keys and passwords for certificate application

A Registration Office shall ensure the delivery of the certificate and the associated private key to the rightful User and attend to their proper protection before delivery. Smart cards, USB tokens and PIN envelopes not yet delivered to the Users shall be kept in a locked cabinet.

When a certificate is delivered on a smart card the associated PIN code shall be delivered in a separate shield envelope.

When a certificate is delivered on a USB token the Registration Officer shall advise the User to change the default PIN code during the first usage time.

When a one-time password is delivered to the user for application and creation of a software certificate the Registration Officer shall ensure that the password is kept secret. If the Registration Officer applies/creates a software certificate on behalf of the User, to be delivered via e-mail, he shall deliver the PIN code via a separate channel.

4. Guidance to Users

Registration Officers shall give adequate guidance to the Users about the usage purposes of their certificates and how to use their private keys. As certificates are a part of the system used to protect the information systems of the organization the Users shall be advised to follow the security instructions and policies of the organization also regarding certificates and private keys. The following security requirements for applying and using certificates shall be emphasized:

- When a User gets a private key into his possession he is from that moment on responsible for protection of his private key and shall prevent it from being lost or compromised or accessible by others.
- The private key shall be protected by a PIN code. A PIN code associated with a software certificate shall comprise at least eight characters including alphabetic, numeric and special characters.
- A PIN code associated with a private key shall be kept secret.
- The User is in person responsible for any operations made using the private key associated with the certificate issued to him, irrespective of if made by the User or by someone else, either without the User's permission or after receiving the PIN code and private key from the User.

The Users shall be advised to submit a notification directly to Sonera's Revocation Service or to the Registration Officer of the User's organization immediately when a User has reason to believe that his private key has been lost or become accessible to someone else, or his PIN code has been compromised, or if the certificate includes information that is no more valid (e.g. User's name has been changed).

5. Revocation of certificates

When a User requires revocation of his certificate the Registration Officer shall always submit a notification for revocation of the certificate to Sonera's Revocation Service. The same applies when the Customer's Administrative Contact Person requires revocation of a User's certificate. The notification shall be submitted also when the Registration Officer has reason to believe that the User's private key or PIN code is not in his sole possession, or it the User does not follow the instructions given to him, based e.g. on this document, concerning usage of certificates and private keys. A notification for revocation shall be submitted also if it is known that the information in a certificate is no more valid, or if the contract between the User and the Customer or between the Customer and Sonera changes or terminates so that the prerequisites for certificate usage cease to exist.

The notification for certificate revocation shall always be submitted immediately upon reason for it becomes evident.

5.1. Revocation of Registration Officer certificates

A Registration Officer shall immediately submit a notification for revocation of his certificate when he has reason to believe that his private key has been lost or become accessible to someone else, or his PIN code has been compromised, or if the certificate includes information that is valid no more (e.g. User's name has been changed).

A Registration Officer shall submit a notification for revocation of the certificate of another Registration Officer when required by the Customer's Administrational Contact Person.