Terms and Conditions of Use of Organisation Certificates (TCU)

Valid from 20.06.2014

DEFINITIONS

Organisation Certificate (certificate) – digital data issued to certify the integrity of a digital document, the link to a digital document, device identification, assurance of secure data transfer, signing of software and/or data encryption, with the public keys thereof uniquely linked to the legal person holding the certificate.

SK – provider of certification services, AS Sertifitseerimiskeskus.
Owner of a Certificate – a legal person whose data has been entered in the certificate.
CP – the Certificate Policy of Organisation Certificates; the rules based on which SK performs the respective certification service (document is published in SK's homepage www.sk.ee, in repository).
CPS - Certification Practice Statement is a framework document that describes the certification practices and procedures used by SK while providing certification services including concepts and procedures connected to the service (document is published in SK's homepage www.sk.ee, in repository).

1. GENERAL TERMS AND CONDITIONS

1.1. SK shall issue certificates to legal persons (hereinafter clients) for digital stamping, digital device identification, assurance of secure data transfer, signing of software and data encryption and provide the service for allowing certificate validity confirmation and the suspension, termination of suspension and revocation of certificates (provision of certification services).

1.2. Web server certificates are issued to clients to whom the domain names of devices belong and/or whose addresses are registered in the respective public databases (in the event that the device is accessible through a public computer network).

1.3. In order to apply for a certificate, the legal representative of the client or a person authorised by them shall submit an electronic application that allows verification of the identify of the representative of the client; by submitting the application, the person certifies the accuracy of the submitted data and assumes full liability for the submission of incorrect data.

1.4. The primary prerequisite for the satisfaction of an application shall be verification of the identities of the legal representatives of the client and the web server device administrator to the application and, if necessary, a positive reply from public databases with regard to the link between a device and the domain name.

1.5. SK shall have the right to amend the Terms and conditions for use of Organisation Certificates and the CP at any time should SK have a justified need for such amendments. Information concerning any amendments shall be published on the website of SK at http://www.sk.ee/.

1.6. The Terms and conditions for use of Organisation Certificates and the CP are binding for the owner of a certificate for the entire term of validity of the certificate and also after the revocation thereof in the event that legal consequences have been caused by activities performed with the formerly valid certificate and the term for contestation thereof has not expired.

2. RIGHTS AND OBLIGA TIONS OF OWNER OF CERTIFICATE

2.1. The owner of a certificate has the right and obligation to use the certificates pursuant to the valid terms and conditions for use of Organisation Certificates and the Digital Signatures Act. SK shall not be liable for any consequences arising from the use of a certificate issued to a client.

2.2. The owner of a certificate shall protect the secret key of the certificate in the best possible manner. The owner of a digital stamp certificate shall preserve the secret key in a secure device for signing (HSM, cryptostick, smart card).

2.3. In the event that the owner of a certificate has lost possession of the secret key of a certificate or there is a danger of the aforesaid event, the owner of a certificate shall immediately submit an application to SK for suspension (only in case of digital stamps) or revocation of the certificate issued to the client.

2.4. The owner of a certificate shall examine the existence of the respective entry in the Certificate Revocation List upon the revocation of a certificate.
2.5. The owner of a certificate shall immediately inform SK of any changes in the contact persons.
2.6. The owner of a certificate undertakes to inform immediately SK of beginning of bankruptcy, liquidation, suspension of operations or other similar state in terms of legislation of its country of origin.
2.7. The owner of a certificate undertakes to inform immediately SK of changes in name and/or IP addresses of the server or device.

3. RIGHTS AND OBLIGATIONS OF SK

3.1. SK shall have the right to refuse to issue a certificate on the bases of CP.
3.2. SK shall have the right to revoke any certificates issued by itself at its own initiative on the bases of the Digital Signatures Act or CP. Certificates will be revoked in following cases:
- If the certificate is not issued on the bases of CP or CPS;
- SK receives a notice of or finds out otherwise that the client has violated one or more significant conditions of TCU and/or CP;
- The client informs SK of the fact that the initial certificate application was not authorised and client does not apply for retroactive authorisation;
- SK finds that control over the client's private key (which corresponds to the certificate's public key) has been lost or it has been compromised;
- If the owner of the certificate has submitted incorrect data or if the data of the owner of a certificate changes substantially and the owner of the certificate has not submitted the request for changes or corrections in data to SK;
- SK receives a notice of or finds out otherwise of circumstances that refer to the fact that the usage of domain name and/or IP address is no longer legal (i.e. the right to use the domain name described in the certificate has been revoked by court order or the contractual relationship between the domain registry has been terminated);
- SK finds out that the certificate has been used for criminal activities such as fraud, spyware, malware and virus distribution, etc.;
- If the owner of a certificate has not paid for the issued certificate within the determined period of time;
- SK terminates its operations in whatever reason and has not delegated the certificate revocation service to another certification service provider;
- There is suspicion that the private key of SK that has been used for signing the certificates has been compromised.

3.3. SK shall submit the refusal to the applicant and the reason for revocation of the certificate(s) to the owner of a certificate in writing.

4. LIABILITY

4.1. The owner of a certificate shall be liable for any damage caused by non-performance or unsatisfactory performance of obligations prescribed in the Terms and conditions for use of Organisation Certificates, the CP and/or the legislation of the Republic of Estonia.
4.2. The owner of a certificate shall be solely and entirely liable for any consequences arising from the use of valid certificates allocated to a client.
4.3. The owner of a certificate is aware that activities performed on the basis of an expired and/or revoked certificate are null and void.
4.4. SK shall not be liable if the owner of a certificate is unable to use the certificates, an interested party is unable to inspect the validity of the certificates or in case other queries/activities cannot be performed for reasons independent of SK (Force majeure, acts or omissions of third parties).
4.5. SK shall be liable for the performance or non-performance of obligations imposed on the provider of certification services by legislation.

5. CERTIFICATE VALIDITY AND VALIDITY CONFIRMATION

5.1. A certificate shall take effect as of the start of the term of validity noted in the certificate, but not before the certificate is entered in the database of valid certificates maintained by SK.

5.2. The validity of a certificate shall end as of the expiry of the term of validity noted in the certificate or upon the revocation of the certificate.

5.3. SK shall suspend (only in case of digital stamp certificates) or revoke the validity of a certificate in the event that it is requested by the owner of the certificate or in case of other grounds provided by legislation.

5.4. SK shall have the right to suspend (only in case of digital stamp certificates) or revoke the validity of a certificate in the event that SK has a reasonable doubt that incorrect data has been entered in the certificate or the owner of a certificate has lost possession of a certificate and it is possible to use the certificate without their permission.

5.5. SK shall immediately inform the owner of a certificate of suspension (only in case of digital stamp certificates) or revocation of the validity of a certificate. In the event that the validity of a certificate was not suspended or revoked by the owner of a certificate, the message shall be communicated to the e-mail address of the contact person of the owner of the certificate.

5.6. The Certificate Revocation List can be used for examining the validity of certificates. Upon inspecting validity on the basis of the Certificate Revocation List, an interested party shall use the newest Revocation List as a basis. The Certificate Revocation List contains suspended and revoked certificates, the time of changing the validity thereof and the reason therefor. Revocation Lists are published periodically every 12 hours on the website of SK at https://www.sk.ee/repositoorium/crl/.

6. PROCESSING OF DATA

6.1. SK shall process personal data of certificate owner according to personal data protection act and other legal acts of Estonian Republic. Principles of client data protection is published at homepage of SK http://www.sk.ee/en/about/data- protection/.

6.2. The owner of a certificate is aware and approves of the fact that their name and registry code are published in the list of valid certificates.

6.3. SK shall have the right to disclose information concerning the owner of a certificate to third parties who’s right to receive information is based on the legislation of the Republic of Estonia.

6.4. The owner of a certificate is aware that, by using certificates for verifying the integrity of a digital document, their certificate containing their name and registry code shall be attached to the digitally verified document.