Conditions for Use of Certificates Issued for Identity Cards, Residence Permit Cards and Digital Identity Cards

Applicable as of 1 December 2014

Definitions

Document (identity card, residence permit card or digital identity card) – an identity card of the Republic of Estonia, issued pursuant to Identity Documents Act.

E-resident digi-ID - digital identification document issued to a person who has no right and need to apply for identity card or residence permit card.

Certificates – digital data in the document allowing digital signature and digital identification. The certificate that allows for digital identification and the certificate that allows for digital signature are connected to the personal data of the user of the document and can be publicly checked against the personal identity code.

SK – AS Sertifitseerimiskeskus, the provider of the certification service.

Certificate owner – the user of the document to whose personal data the digital data in the document pertain.

PINs – security codes used in digital signature and digital identification.

Client service office – service office where applications to receive, suspend, reactivate, revoke or renew certificates or to issue new PINs are received. The list of client service offices can be found on the website http://www.sk.ee/.

Conditions for use – these Conditions for Use of Certificates Issued for Identity Cards, Residence Permit Cards and Digital Identity Cards.

1. General terms and conditions

1.1. SK shall issue certificates to be entered into documents for the purpose of digital identification and digital signature and provide the service that enables checking, renewal, suspension, reactivation and revocation of certificates (provision of the certification service).

1.2. SK shall have a right to make amendments to the conditions for use. Information on the amendments shall be published at http: //www.sk.ee/.

2. Rights and obligations of certificate owners

2.1. Certificate owners have a right and an obligation to use the certificates in compliance with the conditions for use and the Digital Signatures Act.

2.2. Certificate owners shall safeguard their document prudently against anything that may make the certificates in it unusable.

2.3. Certificate owners shall safeguard their PINs in the best possible way. If these have gone out of control of the certificate owner (e.g. these have been stolen), the owner shall immediately change the PINs or if this is not possible, the certificates shall be suspended.

2.4. Certificate owners shall suspend the certificates at a client service office or by calling 1777 (or +372 677 3377) immediately after discovering that the document has been lost. Suspended certificates can be reactivated, new PINs can be applied for (except E-resident digi-ID) and certificates can be revoked only on the basis of a written application submitted to a client service office.

2.5. Upon loss or theft of the document or it becoming unusable due to another reason, the document user shall immediately address the issue to the service of the Police and Border Guard Board for the document to be declared invalid.

3. Responsibility

3.1. Certificate owners shall be solely and fully responsible for any consequences of digital identification and digital signature using their certificates both during and after the validity of the certificates.

3.2. The certificate owner is aware that any digital signature given using expired, suspended or revoked certificates is invalid.

3.3. Certificate owners shall be liable for any damage caused due to failure or undue performance of their obligations specified in the conditions for use and/or Digital Signatures Act.

3.4. SK shall be responsible for performing its obligations specified in legislative acts and liable for failure to perform these.

3.5. SK shall not be liable for circumstances beyond its control (*force majeure*, activity/inactivity of third parties) when certificate owners cannot use digital signature or digital identification, interested parties cannot check the validity of certificates or it is not possible to conduct any other inquiry/operation.

4. Validity of certificates and validity checks

4.1. Certificates become valid as of the date specified in the certificate but not before the certificate has been entered by SK into its database of valid certificates. Certificates of documents are entered into the database of valid certificates within one hour of the issue of the document or reactivation or renewal of the certificates.

4.2. Certificates expire on the date specified in the certificate or when the certificate is revoked. Certificates cease to be valid when the document ceases to be valid.

4.3. SK shall have a right to suspend certificates if it has reasonable doubt that the certificate contains inaccurate data or is out of control of its owner and can be used without owner's permission.

4.4. SK has an obligation to suspend or revoke a certificate if requested by the owner of the certificate or in any other circumstances specified in legislative acts.

4.5. SK shall immediately inform the owner by using @eesti.ee e-mail address that their certificate has been suspended, suspension is terminated or certificate is revoked.

4.6. Validity of certificates can be checked against the revocation list. If an interested party checks the validity of a certificate, they must use the up-to-date revocation list for that. The revocation list contains suspended and revoked certificates, the date when these were suspended or revoked and the basis for that. Revocation lists shall be published at http://www.sk.ee/crls/ regularly and not less than once in every 12 hours.

4.7. Validity of certificates can be checked in the database of valid certificates. This database can be accessed using the LDAP cataloguing service at ldap://ldap.sk.ee/.

5. Processing of personal data

5.1. The certificate owner is aware that their name and personal identification code are processed and published in the database of valid certificates. Expired, suspended or revoked certificates shall not be published in the database of valid certificates.
5.2. The certificate owner is aware and agrees to the fact that during the use of digital certificates in digital identification, the person conducting the identification is sent the certificate that has been entered in their owner's document and contains their name and personal identification code.
5.3. The certificate owner is aware and agrees to the fact that during the use of digital certificates for digital signature, the certificate that has been entered in their document and contains their name and personal identification code is added to the document they digitally sign.
5.4. SK shall process personal data of certificate owner according to personal data protection act and other legal acts of Estonian Republic. Principles of client personal data protection is published at homepage of SK http://www.sk.ee/en/about/data-protection/.
5.5. SK shall have a right to disclose information on certificate owners to third persons who have that right on the basis of the legislative acts of the Republic of Estonia.