CONDITIONS FOR USE OF CERTIFICATES ISSUED FOR DIGITAL IDENTITY CARDS IN THE MOBILE-ID FORM

Applicable as of 01 January 2016

DEFINITIONS

Digital identity card in the form of Mobile-ID (Document) – a digital identity card which Digital authentication certificates and digital signature certificates are related to mobile phone SIM card issued by the Police and Border Guard Board issued under The Identity Documents Act.

Mobile-ID service – a service offered by the mobile network operator allowing the Document user to have access to digital identification and digital signature in an electronic environment.

Mobile-ID SIM – a SIM for mobile phones which enables, in addition to the usual mobile phone usage, the use of the Mobile-ID service and with which the personal data of the Document user is associated.

Mobile network operator – a company engaged in electronic communications that provides mobile communications services and the Mobile-ID service and issues Mobile-ID SIMs to users.

Certificates – digital data associated with the Document and enabling digital identification and digital signature. The digital identification certificates and the digital signature certificates are associated with the personal data of the Document user and can be openly verified with the personal identification code.

SK – AS Sertifitseerimiskeskus, the provider of the certification service. SK accepts digitally signed applications of suspension and termination of suspension of the Mobile-ID certificates

Certificate owner – the user of the Document with whose personal data the digital data in the Document is associated.

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

Client service point – a mobile network operator's service point where the Mobile-ID service contracts are concluded and then the Mobile-ID SIMs are issued, the applications for suspension of Mobile-ID certificates are accepted and changes of the phone numbers associated with the Mobile-ID SIMs are registered. The list of the client service points is available on these websites: http://www.sk.ee/ and the website of the corresponding mobile network operator.

PBGB – the Police and Border Guard Board of the Republic of Estonia, the Document issuer.

PBGB online application environment – the PBGB website (https://www.politsei.ee/en/) where applications can be submitted by those wishing to receive the Document or have it revoked.

Helpline – a round-the-clock phone service provided by the mobile network operator, receiving applications from certificate owners to have their certificates suspended.

Conditions for use – these "Conditions for use of certificates issued for digital identity cards in the Mobile-ID form".

Security area - scraped area on Mobile-ID SIM cover, under which Mobile-ID activation codes (PINs) are located.

1. GENERAL PROVISIONS

1.1. SK issues certificates to be entered into the Document for the purpose of digital identification and digital signature and provides the service that enables checking, suspension, termination of suspension and revocation of certificates (provision of the certification service) according to "Certification Policy of the digital identity card in form of the Mobile-ID" (Certification Policy). Certification Policy is published on the SK website: https://sk.ee/en/repository/CP/.

1.2. SK has the right to amend the Conditions for use whenever necessary. Information about amendments is published on the SK website: https://sk.ee/en.

2. RIGHTS AND OBLIGATIONS OF CERTIFICATE OWNERS

2.1. The certificate owner has the right and the obligation to use the certificates in compliance with the Conditions for use and the laws of the Republic of Estonia.

2.2. The certificate owner has the obligation to refuse to adopt a Mobile-ID SIM card with breached Security area.

2.3. The certificate owner shall safeguard his/hers PINs in the best possible way. In case the PINs have gone out of control of the certificate owner (for instance PINs have been stolen), the owner shall immediately change the PINs or, if this is not possible, have the mobile service and/or certificates suspended.

2.4. Having discovered the loss of the Document and/or PUK code, the certificate owner shall immediately have the mobile service and/or certificates suspended via the round-the-clock Helpline or at a Client service point. The Document and the associated certificates can only be revoked in the PBGB online application environment or at Mobile network operator office which has issued Mobile-ID SIM by submitting an application for termination of the Mobile-ID contract or for exchange of Mobile-ID SIM.

3. RESPONSIBILITY

3.1. The certificate owner shall be solely and fully responsible for any consequences of digital identification and digital signature using the certificates both during and after the validity period of the certificates.

3.2. The certificate owner shall not be responsible for the acts performed during the suspension of certificates. In case certificate owner shall terminate the suspension of certificates, certificate holder will be solely and fully responsible for any consequences arising from digital identification and digital signature using the certificates during the time when the mobile service and/or certificates were suspended. If the certificate owner has a suspicion that the Document has gone out of control of the certificate owner at the time of suspension of mobile service and/or certificates, the certificate owner is obliged to revoke the certificates.

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

3.4. The certificate owner shall be liable for any damage caused due to failure or undue performance of the obligations specified in the Conditions for use and/or the laws of the Republic of Estonia.

3.5. SK shall be responsible for performing its obligations specified in the legislation and liable for failure to perform these.

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

4. CERTIFICATE VALIDITY AND VALIDITY VERIFICATION

4.1. The certificate shall become valid as of the date specified in the certificate.
4.2. The certificate shall expire on the date specified in the certificate or when the certificate is revoked. The certificates are issued with the same validity period as the Document with which they are associated.
4.3. SK has the right to suspend the certificate if SK has reasonable doubt that the certificate contains inaccurate data or is out of the control of its owner and can be used without the owner's permission.
4.4. SK has an obligation to suspend or revoke the certificate if requested by the owner or the mobile network operator or Police and Border Guard Board or on other bases provided by law or legal acts.
4.5. SK shall immediately notify the certificate owner about the certificate suspension, termination of suspension and revocation. The notification shall be sent to the e-mail address of the certificate owner located at @eesti.ee.
4.6. Certificate validity can be checked against the revocation list. If an interested party checks the certificate validity against the revocation list, the party must use the latest versions of the revocation list for the purpose. The revocation list contains the suspended and revoked certificates, the date when these were suspended or revoked and the reason for that. The revocation list is updated and published regularly and not less than once in every 12 hours on the SK website: http://sk.ee/en/repository/CRL/.
4.7. The certificate validity can be checked in the database of valid certificates that can be accessed using the LDAP cataloguing service at ldap://ldap.sk.ee/.

5. PERSONAL DATA PROCESSING

5.1. The certificate owner is aware that its 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 the digital certificates in digital identification, the person conducting the identification is sent the certificate that has been entered in the owner's Document and contains the name and personal identification code of the certificate owner.
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 the Document and contains the name and personal identification code of the certificate owner is added to the document that the owner digitally signs.
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 has the right to disclose information about the certificate owner to a third party who pursuant to relevant laws and legal acts is entitled to receive such information.