Terms and Conditions for Use of Certificates of Personal Identification Documents of the Republic of Estonia

Valid from 03.07.2019

Definitions and Acronyms

Term/Acronym	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
CA	Certificate Authority.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile, rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
CP	Certificate Policy for Mobile ID.
CPS	SK ID Solutions AS – ESTEID-SK Certification Practice Statement.
CRL	Certificate Revocation List.
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
MO	Mobile Operator. Additionally, MO fulfils the role of Telecommunication Service Provider.
Mobile ID	A digital identity document issued pursuant to Identity Documents Act and in a mobile-ID format, the Certificates of which enabling electronic identification and electronic signature are connected to the SIM-card of mobile phone. Mobile ID is issued for some period of time, and contains related QSCD (SIM-card) and several pairs of Certificates consisting of an Authentication Certificate and a Qualified Electronic Signature Certificate.
OCSP	Online Certificate Status Protocol.
OID	An identifier used to uniquely name an object.
PIN code	Activation code for a Private Key.
PBGB	Police and Border Guard Board.
Private Key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
QSCD	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation. In the context of Mobile ID, QSCD compliant SIM-card is a QSCD.
Qualified Certificate	A certificate for electronic signatures, that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of eIDAS Regulation.
Qualified Electronic Signature	Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a Qualified Certificate for electronic signatures.
Relying Party	Entity that relies on the information contained within a Certificate.
SK	SK ID Solutions AS
SK PS	SK ID Solutions AS Trust Services Practice Statement.
SLA	Service Level Agreement.
Subscriber	A natural person to whom the Certificates of Mobile-ID are issued as a public service if he/she has a statutory right.
Terms and Conditions	Present document that describes the obligations and responsibilities of the Subscriber while using the Certificates.

1. **General Terms**
   1.1. Present Terms and Conditions describe main policies and practices followed by SK and provided in CP, CPS and SK PS (e.g. Disclosure Statement).
   1.2. The Terms and Conditions govern the Subscriber's use of the Certificates and constitute a legally binding contract between the Subscriber and SK.
   1.3. The Subscriber has to be familiar with the Terms and Conditions and accept them upon receipt of the Certificates.
   1.4. SK has the right to amend the Terms and Conditions at any time should SK have a justified need for such amendments. Information on the amendments shall be published on the website https://sk.ee/en.
2. **Certificate Acceptance**
   2.1. In case Certificates for Mobile ID are issued or QSCD is replaced i.e. Certificate re-key is performed:
      2.1.1. SK issues Mobile ID Certificates and notifies PBGB and MO of the new Certificate issuance to the Subscriber. PBGB or MO notifies the Subscriber of the new Certificate issuance and respective notification is deemed Certificate acceptance.
3. **Certificate Type, Validation Procedures and Usage**

Certificate Type	Usage	Certification Policy Applied and Published	OID	Summary
Certificates for Mobile ID	Qualified Electronic Signature Certificate is intended for: Creating Qualified Electronic Signatures compliant with eIDAS [9].	SK ID Solutions AS – Certificate Policy for Mobile ID of the Republic of Estonia, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.1.3	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) SK attribute in IANA register (10015) Certification service attribute (1.3)
		ETSI EN 319 411-2 Policy: QCP-n-qscd	0.4.0.194112.1.2	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd(2)

	Authentication Certificate is intended for: Authentication, secure e-mail	SK ID Solutions AS – Certificate Policy for Mobile ID of the Republic of Estonia, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.1.3	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) SK attribute in IANA register (10015) Certification service attribute (1.3)
		ETSI EN 319 411-1 Policy: NCP+	0.4.0.2042.1.2	itu-t(0) identified-Organisation(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

3.1. The use of the Subscriber´s Certificates is prohibited for any of the following purposes:

3.1.1. Unlawful activity (including cyber attacks and attempt to infringe the Certificate, or Mobile ID)

3.1.2. Issuance of new Certificates and information regarding Certificate validity

3.1.3. Enabling other parties to use the Subscriber's Private Key

3.1.4. Enabling the Certificate issued for electronic signing to be used in an automated way

3.1.5. Using the Certificate issued for electronic signing for signing documents which can bring about unwanted consequences (including signing such documents for testing purposes)

3.2. The Subscriber Authentication Certificate can not be used to create Qualified Electronic Signatures compliant with eIDAS.

4. **Reliance Limits**

4.1. Certificates become valid as of the date specified in the Certificate.

4.2. Certificates become invalid on the date specified in the Certificate or when the Certificate is suspended or revoked. Certificates cease to be valid when ceases to be valid.

4.3. Audit logs are retained on-site for no less than 10 years. Physical or digital archive records regarding Certificate applications, registration information and requests or applications for suspension, termination of suspension and revocation are retained for at least 10 years after the expiry of the relevant Certificate.

5. **Subscriber's Rights and Obligations**

5.1. The Subscriber has the right to submit an application for issuing the Certificate.

5.2. The Subscriber is obligated to:

5.2.1. Accept the Terms and Conditions

5.2.2. Adhere to the requirements provided by SK

5.2.3. Use his/her Private Key solely for creating Qualified Electronic Signatures

5.2.4. Use his/her Private Key and Certificate in accordance with Terms and Conditions, including applicable agreements set out in art. 9, and the laws of the Republic of Estonia and European Union

5.2.5. Ensure that he/she no longer uses his/her Private Key, in the case of being informed that his/her Certificate has been revoked or that the issuing CA has been compromised

5.2.6. Ensure that the Subscriber´s Private Key is used under his/her control

5.3. The Subscriber is obligated to present true and correct information to PBGB while submitting an application for Mobile ID Certificates.

5.4. The Subscriber is obligated to present true and correct information to MO:

5.4.1. While submitting an application for QSCD or for change of QSCD or

5.4.2. While submitting an application for replacement of QSCD

5.4.3. While submitting an application for Certificates for valid Mobile ID (Certificate re-key)

5.5. The Subscriber is aware that SK publishes his/her valid Certificates during their validity period via LDAP directory service.

5.6. In case of a change in personal details, the Subscriber is obligated to immediately notify PBGB of the correct details in accordance with the established legislation.

5.7. The Subscriber is obligated to apply for a new QSCD and Mobile ID Certificates, in case of a change in his/her personal details stored in the Certificate and in order to continue usage of Mobile ID service.

5.8. In case Mobile ID is lost, stolen, unusable or destroyed, the Subscriber is obligated to:

5.8.1. Notify MO or PBGB in accordance with the effective legislation

5.8.2. Revoke the Certificates, if the Subscriber has a suspicion that his/her Mobile ID has gone out of his/her control at the time of suspension of telecommunications service and/or Certificate

5.9. Mobile ID and Certificates can be revoked in PBGB online application environment or by calling MO Help Line or at MO´s Customer Service Points which has issued Mobile ID SIM-card by submitting an application for termination of the Mobile ID contract or for exchange of Mobile ID SIM-card.

6. **SK's Rights and Obligations**

6.1. SK has the right to suspend Certificates if it has reasonable doubt that the Certificate contains inaccurate data or Private Key is out of control of its owner and can be used without the Subscriber's permission.

6.2. While providing certification service for Mobile ID SK is obligated to:

6.2.1. Supply the certification service in accordance with the applicable agreements set out in art 9 and relevant legislation

6.2.2. Keep account of the Certificates issued by it and of their validity

6.2.3. Accept applications for suspension of Certificates 24 hours a day

6.2.4. Provide the possibility to check the validity of Certificates on its website 24 hours a day

6.2.5. Provide security with its internal security procedures

6.2.6. Suspend or revoke a Certificate if requested by the Subscriber, PBGB or MO or under any other circumstances specified in laws or legal acts

6.2.7. Inform the owner by using @eesti.ee e-mail address that their Certificate has been suspended, suspension has been terminated or Certificate has been revoked

6.2.7.1. Accept and register the issuance of the QSCD-s and corresponding Public Keys presented by MO

6.2.7.2. Accept and register the Certificate requests presented by PBGB and issue the corresponding Certificates

6.2.7.3 Accept and register the requests of the Certificates presented by MO, verify validity of the QSCD to be replaced and previously issued Certificates (in case of Certificate re-key) and decide the issuance of the Certificates and forward the information on issuance of Certificates to PBGB

6.2.7.4. Accept, register and process the applications for revocation of Mobile ID Certificates presented by MO and forward the information on revocation of the Certificates to PBGB

7. **Certificate Status Checking Obligations of Relying Parties**

7.1. A Relying Party shall study the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in the CPS and the CP.

7.2. If not enough evidence is enclosed to the Certificate or Qualified Electronic Signature with regard to the validity of the Certificate, a Relying Party shall verify the validity of the Certificate on the basis of certificate validation services offered by SK at the time of using the Certificate or affixing a Qualified Electronic Signature.

7.3. A Relying Party shall follow the limitations stated within the Certificate and makes sure that the transaction to be accepted corresponds to the CPS and CP.

7.4. SK ensures availability of Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99.44% availability overall per year with a scheduled down-time that does not exceed 0.28% annually.

7.5. SK offers OCSP service for checking Certificate status. Service is accessible over HTTP protocol.

7.6. A Relying Party shall verify the validity of the Certificate by checking Certificates validity against OCSP. SK offers OCSP with following checking availability:

7.6.1. An OCSP service is free of charge and publicly accessible at http://aia.sk.ee/esteid2015

7.6.2. SK offers an OCSP service with better SLA under agreement and price list

7.6.3. OCSP contains Certificate status information until the Certificate expires

7.7. Additionally SK offers CRL service for checking Certificate status. Service is accessible over HTTP protocol. SK offers CRL with following checking availability:

7.7.1. If a Relying Party shall check Certificate validity against the CRL, the Party must use the latest versions of the CRL for the purpose

7.7.2. The CRL contains the revoked Certificates, the date and reasons for revocation

7.7.3. The value of the nextUpdate field of CRL is set to 12 hours after CRL issuance

7.7.4. A valid CRL is free of charge and accessible on the website https://www.sk.ee/en/repository/CRL/

7.7.5. Relying Party shall use CRL service on its own responsibility

7.7.6. The URLs of the services are included in the Certificates on the CRL Distribution Point (CDP) and Authority Information Access (AIA) fields respectively in accordance with the Certificate Profile. The URLs of the CDP is included in the Certificates issued until 31.10.2021

7.8. Revocation status information of the expired Certificate can be requested at the email address info@sk.ee

8. **Limited Warranty and Disclaimer/Limitation of Liability**

8.1. The Subscriber is solely responsible for the maintenance of his/her Private Key.

8.2. The Subscriber is solely and fully responsible for any consequences of Authentication and Electronic Signature using their Certificates both during and after the validity of the Certificates.
8.3. The Subscriber is solely liable for any damage caused due to failure or undue performance of his/her obligations specified in the Terms and Conditions and/or the laws of the Republic of Estonia.
8.4. The Subscriber is aware that Electronic Signatures given on the basis of expired, revoked or suspended Certificates are invalid.
8.5. The Subscriber is not responsible for the acts performed during the suspension of Certificates. In case the Subscriber terminates suspension of Certificates, the Subscriber is solely and fully responsible for any consequences of Authentication and Qualified Electronic Signature using the Certificates during the time when the Certificates were suspended.
8.6. SK ensures that:
8.6.1. The certification service is provided in accordance with CPS, CP and the relevant legislation of the Republic of Estonia and European Union
8.6.2. Certificates are revoked immediately after the request's legality has been verified. The revocation of the Certificate is recorded in the Certificate database of SK and in CRL no later than 24 hours after an application has been submitted
8.6.3. The certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK
8.6.4. The certification keys used to provide the certification service are activated on the basis of shared control
8.6.5. It has compulsory insurance contracts covering all SK services to ensure compensation for damages caused by SK's breach of obligations
8.6.6. It informs all Subscribers before SK terminates service of Certificates and maintains the documentation related to the terminated service of Certificates and information needed according to the process set out in CPS
8.7. SK is not liable for:
8.7.1. The secrecy of the Private Keys of the Subscribers, any misuse of the Certificates or inadequate checks of the Certificates or for the wrong decisions of a Relying Party or any consequences due to error or omission in Certificate validation checks
8.7.2. The non-performance of its obligations if such non-performance is due to faults or security problems of the supervisory body, the data protection supervision authority, Trusted List or any other public authority
8.7.3. The failure to perform if such failure is occasioned by force majeure.

9. **Applicable Agreements, CPS, CP**

9.1. Relevant agreements, policies and practice statements related to Terms and Conditions for use of Certificates are:
9.1.1. SK ID Solutions AS – Certificate Policy for Mobile ID of the Republic of Estonia, published at: https://sk.ee/en/repository/CP/
9.1.2. SK ID Solutions AS – ESTEID-SK Certification Practice Statement, published at: https://sk.ee/en/repository/CPS/

9.1.3. SK ID Solutions AS - Trust Services Practice Statement, published at: https://sk.ee/en/repository/sk-ps/

9.1.4. Certificate, CRL and OCSP Profile for Personal Identification Documents of the Republic of Estonia, published at: https://sk.ee/en/repository/profiles/

9.1.5. Principles of Processing Personal Data, published at: https://sk.ee/en/repository/data-protection/

9.2. Current versions of all applicable documents are publicly available in SK repository: https://sk.ee/en/repository/

10. **Privacy Policy and Confidentiality**

10.1. SK follows the Principles of Processing Personal Data, provided in SK repository https://sk.ee/en/repository/data-protection/ and other legal acts of Estonian Republic, when handling personal information and logging information.

10.2. The Subscriber is aware and agrees to the fact that during the use of his/her Authentication Certificate in Authentication, the corresponding Certificate that contains the Subscriber´s name and personal identification code is sent to the person conducting the Authentication.

10.3. The Subscriber is aware and agrees to the fact that during the use of his/her Qualified Electronic Signature Certificate for Qualified Electronic Signature, the corresponding Certificate that contains the Subscriber's name and personal identification code is added to the document he/she electronically signs.

10.4. All information that has become known while providing services and that is not intended for disclosure (e.g. information that had been known to SK because of operating and providing Trust Services) is confidential. The Subscriber has the right to obtain information from SK about him/herself pursuant to the law.

10.5. SK secures confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties by implementing different security controls.

10.6. SK has the right to disclose information about the Subscriber to a third party who pursuant to relevant laws and legal acts is entitled to receive such information.

10.7. SK is entitled to perform checks from reliable sources related to the Subscriber's identity validation should SK consider it necessary for the purpose of providing certification service.

10.8. Non-personalised statistical data about SK's services is also considered public information. SK may publish non-personalised statistical data about its services.

10.9. The registration information is retained for 10 years after the end of the Certificate validity period.

11. **Refund Policy**

11.1. SK handles refund case-by-case.

12. **Applicable law, complaints and dispute resolution**

12.1. The certification service is governed by the jurisdictions of Estonia and European Union as the location where SK is registered as a CA.

12.2. All disputes between the parties will be settled by negotiations. If the parties fail to reach an amicable agreement, the dispute will be resolved at the court of the location of SK.

12.3. The other parties will be informed of any claim or complaint not later than 30 calendar days after the detection of the basis of the claim, unless otherwise provided by law.

12.4. The Subscriber or other party can submit their claim or complaint on the following email: info@sk.ee.

12.5. All dispute requests should be sent to contact information provided in these Terms and Conditions.

13. **SK and Repository Licences, Trust Marks and Audit**

13.1. The certification service for Qualified Electronic Signature Certificate for Mobile ID has qualified status in the Trusted List of Estonia: https://sr.riik.ee/tsl/estonian-tsl.pdf. The prerequisite requirement of thisregistration is compliance with applicable regulations and standards.

13.2. The conformity assessment body is accredited in accordance with Regulation (EC) No 765/2008 as competent to carry out conformity assessment of the qualified Trust Service Provider and qualified Trust Services it provides.

13.3. Audit conclusions or certificates, which are based on audit results of the conformity assessment conducted pursuant to the eIDAS Regulation, corresponding legislation and standards are published on SK's website https://www.sk.ee/en/repository/.

14. **Contact Information**

14.1. Trust Service Provider
SK ID Solutions AS
Registry code 10747013
Pärnu Ave 141, 11314 Tallinn, ESTONIA
(Mon-Fri 9.00 a.m. - 6.00 p.m. Eastern European Time)
http://www.sk.ee/en
Phone +372 610 1880
Fax +372 610 1881
E-mail: info@sk.ee

14.2. Revocation and suspension requests of Mobile ID are accepted at:

14.2.1. Suspension: at MO's Customer Service Points or 24/7 by calling MO Help Line at:

- 123
- +372 6600 600
- +372 6 866 866

14.2.2. Revocation: PBGB online application environment or by calling MO Help Line at +372 6 866 866 or at MO´s Customer Service Points;

14.3. The list and contact details of MO Customer Service Point can be checked on SK's website https://sk.ee/en/kontakt/customerservice/ and MO;

14.4. The list and operating hours of PBGB's or SK's Customer Service Points can be checked on the websites of PBGB and SK: https://www.politsei.ee/en/kontakt/kmb/ and https://sk.ee/en/kontakt/customerservice/.