Terms and Conditions for Use of Certificates of Mobile-ID of Lithuania

Valid from 24.10.2018

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	SK ID Solutions AS - Certificate Policy for Mobile-ID of Lithuania.
CPS	SK ID Solutions AS – EID-SK Certification Practice Statement.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
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 form of digital identity, the Certificates of which enabling electronic identification and electronic signature are connected to the SIM-card of Mobile phone.
OCSP	Online Certificate Status Protocol.
OID	An identifier used to uniquely name an object.
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.
Qualified Electronic Signature Creation Device (QSCD)	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation.
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 or Certificate status information provided by SK.
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.

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 for Mobile-ID, CPS and SK PS (e.g. Disclosure Statement).

1.2 The Terms and Conditions govern Subscribers' use of the Certificates and constitute a legally binding contract between 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.

1.5 The Subscriber can apply for Mobile-ID only personally. Mobile-ID cannot be issued to a representative.

2 **Certificate Acceptance**

2.1 Upon signing a Mobile-ID agreement, the Subscriber confirms that he/she is familiar with and accepts the Terms and Conditions. Corresponding confirmation is deemed Certificate acceptance for Mobile-ID.

2.2 If the Certificate re-key is performed the Subscriber confirms that he/she has read and agrees to the Terms and Conditions.

3 **Certificate Type, Validation Procedures and Usage**

Certificate Type	Usage	Certification Policy Applied and Published	OID	Summary
Certificates for Mobile-ID Certificate	Qualified Electronic Signature Certificate is intended for: creating Qualified Electronic Signatures compliant with eIDAS.	SK ID Solutions AS – Certificate Policy for Mobile-ID of Lithuania, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.18.1	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.	SK ID Solutions AS – Certificate Policy for Mobile-ID of Lithuania, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.18.1	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 revoked.

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 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 for Mobile-ID.

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 Keys solely for creating Qualified Electronic Signatures;
5.2.4 use his/her Private Key and Certificate in accordance with the 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 Subscriber´s Private Key is used under his/her control;
5.2.7 present true and correct personal data to MO;
5.2.8 notify MO in case of Mobile-ID becoming unusable, lost or destroyed in accordance with the effective legislation;
5.2.9 in case of a change in his/her personal details stored in the Certificate to apply for a new QSCD and Mobile-ID Certificates in order to continue usage of the Mobile-ID service;
5.2.10 immediately inform SK of a possibility of unauthorised use of his/her Private Key and revoke his/her Certificates;
5.2.11 immediately revoke his/her Certificates if his/her Private Key has gone out of his/her possession or the device has been stolen.

5.3 The Subscriber is aware that Electronic Signatures given on the basis of expired or revoked Certificates are invalid.

6 SK's Rights and Obligations

6.1 SK is obligated to:
6.1.1 supply certification service in accordance with the applicable agreements set out in art. 9 and relevant legislation;
6.1.2 keep account of the Certificates issued by it and of their validity;
6.1.3 provide security with its internal security procedures;
6.1.4 provide the possibility to check the validity of Certificates 24 hours a day;
6.1.5 accept and register batches of Public Keys presented by MO;
6.1.6 accept and register the issuance of QSCD-s and corresponding Public Keys presented by MO;
6.1.7 accept and register the requests of the Certificates presented by MO and decide the issuance of the Certificates;
6.1.8 accept, register and process the applications for revocation of Mobile-ID Certificates presented by the Subscriber, MO and competent authority;
6.1.9 provide the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK;
6.1.10 provide the certification keys used in the supply of the certification service are activated on the basis of shared control.

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 downtime 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 OCSP service is free of charge and publicly accessible at http://aia.sk.ee/eid2016;
7.6.2 SK offers an OCSP service with better SLA under agreement and price list;
7.6.3 OCSP service contains Certificate status information until the Certificate expires;
7.6.4 The URL of the OCSP service is included in the certificate on the Authority Information Access (AIA) field in accordance with the Certificate Profile.

7.7 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 or revoked Certificates are invalid.
8.5 SK ensures that:
8.5.1 the certification service is provided in accordance with CPS, CP and the relevant legislation of the Republic of Estonia and European Union;
8.5.2 the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK;
8.5.3 the certification keys used to provide the certification service are activated on the basis of shared control;
8.5.4 it has compulsory insurance contracts covering all SK services to ensure compensation for damages caused by SK's breach of obligations;
8.5.5 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.
8.6 SK is not liable for:
8.6.1 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;
8.6.2 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;
8.6.3 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 the Terms and Conditions are:

9.1.1 SK ID Solutions AS – Certificate Policy for Mobile-ID of Lithuania, published at https://sk.ee/en/repository/CP/;

9.1.2 SK ID Solutions AS – EID-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 and OCSP Profile for Mobile-ID of Lithuania, published at: https://sk.ee/en/repository/profiles/;

9.1.5 Principles of Client Data Protection, 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 Client Data Protection, 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 Certificates for Authentication, the person conducting Authentication is sent the Certificate that has been issued to the Subscriber and contains their name and personal identification code.

10.3 The Subscriber is aware and agrees to the fact that during the use of Certificates for Qualified Electronic Signature, the Certificate that has been issued to the Subscriber and contains their name and personal identification code is added to the document they electronically sign.

10.4 All information that has become known while providing services and that is not intended for disclosure (e.g. information that has been known to SK due to 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 is entitled 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 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 shall be settled by negotiations. If the parties fail to reach an amicable agreement, the dispute shall be resolved at the court of the location of SK.

12.3 The other parties shall 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 at 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/en/tl.html. The prerequisite requirement of this registration 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://sk.ee/en/repository/audit/.

14 Amendments

14.1 All amendments regarding Mobile-ID are coordinated with MO.

14.2 Amended Terms and Conditions are published electronically at: https://www.sk.ee/en/repository/conditions-for-use-of-certificates/.

15 Contact Information

15.1 Trust Service Provider

SK ID Solutions AS

Registry code 10747013

Pärnu Ave 141, 113134

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

15.2. The requests for suspension of the telecommunication service are accepted 24/7 via MO Help Line. MO Help Line may be contacted at:

15.2.1 1817 or 8 698 63 333;

15.2.2 1501;

15.2.3 1575 or 117; +370 6 840 0075 or +370 6 840 0117;1577; +370 6 840 0077.

15.3 The applications for revoking Mobile-ID Certificates are accepted at MO Customer Service Points.

15.4. 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's website.