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

Valid from 01.11.2016

1.Definitions and Acronyms

Term/Acronym	Definition
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 ID card and/or Digi-ID and/or Mobile-ID.
CPS	AS Sertifitseerimiskeskus – ESTEID-SK Certification Practice Statement.
CRL	Certificate Revocation List.
Document	An identity document of the Republic of Estonia, issued pursuant to Identity Documents Act, e.g (ID card, Digi-ID, Mobile ID).
Digi-ID	Digital identity document, issued pursuant to Identity Documents Act to an Estonian citizen and an alien who has been issued an identity card or residence permit card before or who is applying for an identity card or residence permit card concurrently with the digital identity card or to an e-resident.
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.
E-resident	An alien who has a relationship with the Estonian state or legitimate interest in the use of e-services of the Estonian state but who is not Estonian citizen nor resident.
IDA	Identity Documents Act.
ID card	An identity document which is a mandatory identity document of the Estonian citizens and aliens staying/residing permanently in Estonia and issued pursuant to Identity Documents Act.
MO	Mobile Operator.
Mobile ID	A digital identity document issued pursuant to Identity Documents Act, 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.
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.
Relying Party	Entity that relies on the information contained within a Certificate.
RP card	A residence card issued from year 2011 to natural persons entitled by IDA is a mandatory identity document of an alien who is residing permanently in Estonia on the basis of a valid residence permit or right of residence. In this document is referred to as ID card. Estonian residence permit is not the same as EU residence permit.
SK	AS Sertifitseerimiskeskus, a provider of certification services.
SK PS	AS Sertifitseerimiskeskus Trust Services Practice Statement.
SLA	Service Level Agreement.
Subscriber	A natural person to whom the Certificates of ID card, Digi-ID or 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.
Trüb Baltic AS	Manufacturer of ID cards. Additionally, Trüb Baltic AS prepares Digi-ID blanks in the factory and provides technical environment for personalisation in RA office.

1 **General Terms**

1.1 Present Terms and Conditions describe main policies and practices followed by SK and provided in CP for the ID card, CP for the Digi-ID, CP for the 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 SK issues Certificates to natural persons or to natural person's representative entitled by IDA, except Mobile ID, which cannot be issued to a representative.

2 **Certificate Acceptance**

2.1 In case of ID card and Digi-ID Certificates issuance:

2.1.1 Acceptance of and signing the Terms and Conditions as well as confirmation that the ID card or Digi-ID has been handed over to the Subscriber are deemed Certificate acceptance.

2.2 In case of ID card and Digi-ID Certificate re-key and modification:

2.2.1 If the Certificate re-key or modification is performed to fix production errors, rekey in order to replace an expired or broken ID card or Digi-ID, modification to change data visually imprinted on the ID card or Digi-ID and stored in the Personal Data File, the Subscriber confirms that he/she has read and agrees to the Terms and Conditions as stated in clause 3.1.1.

2.2.2 The Certificate re-key and modification to fix ASN.1 encoding errors in Certificates or replace SHA-1 signatures, modification to change e-mail addresses written to Subject Alternative Name field of the Authentication certificate can be requested in public data network in case the Authentication Certificate of the ID card or Digi-ID is valid and in active state or at PBGB Customer Service Point. If the Certificate re-key or modification is performed:

2.2.2.1 In an application in public data network, the Subscriber is notified of the issuance of the new Certificate by the application. Notification by the application is deemed acceptance of a re-keyed or modified Certificate.

2.2.2.2 At PBGB Customer Service Point, the Subscriber is notified of the issuance of the new Certificate by an employee of PBGB Customer Service Point. Notification by an employee of PBGB Customer Service Point is deemed acceptance of a re-keyed or modified Certificate.

2.3 In case of Mobile ID Certificate issuance or QSCD replacement (re-key):

2.3.1 SK issues the Mobile ID Certificates and notifies MO of the new Certificate issuance to the Subscriber. 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 ID card	Qualified Electronic Signature Certificate is intended for: creating Qualified Electronic Signatures compliant with eIDAS	AS Sertifitseerimiskeskus – Certificate Policy for the ID card, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.1.1	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(1.1)
		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, Encryption, secure e-mail	AS Sertifitseerimiskeskus – Certificate Policy for the ID card, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.1.1	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(1.1)
		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)
Certificates for Digi-ID	Qualified Electronic Signature Certificate is intended for: creating Qualified Electronic Signatures compliant with eIDAS	AS Sertifitseerimiskeskus – Certificate Policy for Digi-ID, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.1.2	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(1.2)
		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, Encryption, secure e-mail	AS Sertifitseerimiskeskus – Certificate Policy for Digi-ID, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.1.2	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(1.2)
		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)
Certificates for Mobile-ID Certificate	Qualified Electronic Signature Certificate is intended for: creating Qualified Electronic Signatures compliant with eIDAS [9].	AS Sertifitseerimiskeskus – 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	AS Sertifitseerimiskeskus – 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 the ID card, Digi-ID, 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. Certificates cease to be valid when the document 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 the requirements provided by SK;
- 5.2.3 use his/her Private Key and Certificate in accordance with Terms and Conditions, including applicable agreements set out in art. 10, and the laws of the Republic of Estonia and European Union;
- 5.2.4 ensure that Subscribers´s Private Key is used under its control.

5.3 The Subscriber is obligated to present true and correct information to PBGB:
- 5.3.1 upon application for the ID Card and Digi-ID or;
- 5.3.2 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 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.

5.6 The Subsciber is obligated to apply for 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.

5.7 Subscriber´s obligations in case of the loss or unauthorised use of ID card or Digi ID:
- 5.7.1 Having discovered the loss of ID card or Digi ID or the possibility of unauthorised use of his/her Private key, the Subscriber is obligated to immediately suspend the Certificates by calling 1777 (or +372 677 3377) or at a Customer Service Point. Suspended Certificates can be reactivated and new PINs can be applied for (except E-resident digi-ID);
- 5.7.2 The Subscriber is obligated to revoke the Certificates, if the Subscriber has a suspicion that the ID Card or Digi-ID has gone out of control of the Subscriber at the time of suspension of Certificates;
- 5.7.3 Certificates can be revoked only on the basis of a written application submitted to a Customer Service Point.

5.8 Subscriber´s obligations in case Mobile ID is lost, unusable or destroyed:
- 5.8.1 Having discovered that Mobile ID has been lost, destroyed or become unusable, the Subscriber is obligated

. immediately suspend Certificates via the MO´s round the clock helpline or at a MO´s Customer Service Points;

5.8.2 If the Subscriber has a suspicion that Mobile ID has gone out of control of the Subscriber at the time of suspension . of telecommunications service and/or Certificate, the Subscriber is obliged to revoke the Certificates;

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

5.9 Upon loss or theft of the Document or it becoming unusable due to another reason, the Subscriber is obligated to . immediately address the issue to the service of the PBGB for the document to be declared invalid.

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 is out of . control of its owner and can be used without Subscriber's permission.

6.2 While providing certification service for ID card, Digi-ID, Mobile ID SK is obligated to:

. 6.2.1 supply the certification service in accordance with the applicable agreements set out in art 10 and relevant . legislation;

6.2.2 keep account of the Certificates issued by it and of their validity;

6.2.3 accepts applications for suspension of Certificates 24 hours a day;

6.2.4 it provides the possibility to check the validity of certificates on its website 24 hours a day;

6.2.5 it provides security with its internal security procedures;

6.2.6 suspend or revoke a Certificate if requested by the Subscriber of the Certificate, PBGB, MO (in case of . Mobile ID) 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 is . terminated or Certificate is revoked.

6.3 While providing certification service for Mobile ID service SK is additionally obligated to:

. 6.3.1 accept and register the issuance of the QSCD-s and corresponding Public Keys presented by MO;

6.3.2 accept and register the Certificate requests presented by PBGB and issue the corresponding Certificates;

6.3.3 accept and register the requests of the Certificates presented by MO (in case of Certificate re-key) and decide the . issuance of the Certificates and forward the information on issuance of Certificates to PBGB;

6.3.4 accept, register and process applications presented by MO for revocation of Mobile ID certificates;

6.3.5 it accepts, registers and processes the applications for revocation of Mobile ID certificates presented by MO and . forwards the information on revocation of the certificates to PBGB.

7 Certificate Status Checking Obligations of Relying Parties

. 7.1 Relying Party studies 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 verifies 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 follows 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 Relying Party verifies 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.

7.7 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 checks 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 uses 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.

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 digital identification and digital 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 conditions for use and/or the laws of the Republic of Estonia.

8.4 The Subscriber is aware that digital 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 Sertifitseerimiskeskus – Certificate Policy for the ID card, published at https://sk.ee/en/repository/CP/;

9.1.2 AS Sertifitseerimiskeskus – Certificate Policy for Digi-ID, published at https://sk.ee/en/repository/CP/;

9.1.3 AS Sertifitseerimiskeskus – Certificate Policy for Mobile ID of the Republic of Estonia, published at https://sk.ee/en/repository/CP/;

9.1.4 AS Sertifitseerimiskeskus – ESTEID-SK Certification Practice Statement, published at https://sk.ee/en/repository/CPS/;

9.1.5 AS Sertifitseerimiskeskus Trust Services Practice Statement, published at: https://sk.ee/en/repository/sk-ps/;

9.1.6 Certificate, CRL and OCSP Profile for personal identification documents of the Republic of Estonia, published at: https://sk.ee/en/repository/profiles/

9.1.7 Principles of Client Data Protection https://sk.ee/en/repository/data-protection/.

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

10 Privacy Policy and Confidentiality

10.1 SK follows the Principles of Client Data Protection, provided in the 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 in digital identification, the person conducting the identification is sent the Certificate that has been entered in Subscriber´s Document and contains Subscriber´s name and personal identification code.

10.3 The Subscriber is aware and agrees to the fact that during the use 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.

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

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

11 Refund Policy

11.1 The Subscriber is entitled to apply for the refund of the state fee for the review of an application for the issuance of the ID card and Digi-ID in accordance with the Estonian State Fees Act.

11.2 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 ID card, Digi-ID and Mobile ID format has qualified status in the Trusted List of Estonia: https://sr.riik.ee/en/tsl/estonia.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://www.sk.ee/en/repository/.

14 Amendments

14.1 All amendments regarding ID-card and/or Digi-ID are coordinated with PBGB as well as Trüb baltic AS. All amendments regarding Mobile ID are coordinated with PBGB and 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

AS Sertifitseerimiskeskus

Registry code 10747013

Pärnu mnt. 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 Revocation and Suspension requests of ID card and Digi-ID are accepted 24/7 at:

15.2.1 Suspension: Phone +1777 (or +372 677 3377) or Customer Service Point or revoke@sk.ee;

15.2.2 Revocation: Customer Service Point.

15.3 The most recent contact details are available at SK's website: https://sk.ee/en/kontakt/customerservice/.

15.4 Revocation and Suspension request of Mobile ID are accepted are accepted 24/7 at:

15.4.1 Suspension: MO´s round the clock helpline or at a MO´s Customer Service Points or revoke@sk.ee, which accepts electronically signed applications of suspension and termination of suspension of Mobile ID Certificates;

15.4.2 Revocation: PBGB online application environment or at MO´s Customer Service Points;

15.5 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;

15.6 The list and operating hours of PBGB Customer Service Points can be checked on the websites of PBGB and SK: https://www.politsei.ee/en/kontakt/kmb/ and http://www.vm.ee/en/country-representations/estonian-representations and https://sk.ee/en/kontakt/customerservice/.