Terms and Conditions for Use of Certificates of SEB-card

Valid from: 24.10.2018

Definitions and Acronyms

Term/Acronym	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
Authentication Certificate	Certificate is intended for Authentication and encryption.
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.
Certificate Authority (CA)	A part of SK structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
CP	SK ID Solutions AS - Certificate Policy for the SEB card.
CPS	SK ID Solutions AS – EID-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.
OCSP	Online Certificate Status Protocol.
OID	An identifier used to uniquely name an object.
PIN code	Activation code for the Authentication Certificate and for the Qualified Electronic Signature Certificate.
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	Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a Qualified Certificate for electronic signatures.
QSCD	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation.
Relying Party	Entity that relies on the information contained within a Certificate.
SEB	AS SEB Pank. Legal body tasked with issuing SEB-cards to natural persons.
SEB-card	Employee card issued by SEB linked to Certificates facilitate electronic signatures and electronic identification of natural persons. These documents are not deemed identity documents in the legal sense.
SK	SK ID Solutions AS, a provider of certification services.
SK PS	SK ID Solutions AS Trust Services Practice Statement.
SLA	Service Level Agreement.

Subscriber	A natural person to whom the Certificates of SEB-card 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 the SEB card, 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 and accept the Terms and Conditions.

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 will be published in the SEB intranet and on SK´s website https://sk.ee/en.

1.5 The Subscriber cannot apply for SEB-card through a representative and SEB-card cannot be issued to a representative.

2 **Certificate Acceptance**

2.1 Acceptance of and signing the Terms and Conditions as well as confirmation that the SEB-card has been handed over to the Subscriber are deemed Certificate acceptance for SEB-card.

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 SEB-card	Qualified Electronic Signature Certificate is intended for: creating Qualified Electronic Signatures compliant with eIDAS.	SK ID Solutions AS – Certificate Policy for the SEB card, published https ://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.13.1	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(13.1)
		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, secure e-mail, Smart Card logon to the workstation.	SK ID Solutions AS – Certificate Policy for the SEB card, published https ://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.13.1	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(13.1)
		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)

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 SEB card);

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 The validity of the Certificate expires on the date of expiry indicated in the Certificate or if 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 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 for SEB-card.

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 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 Subscribers´s Private Key is used under its control;

5.2.7 present true and correct information;

5.2.8 protect his/her PIN codes to the best of his abilities. If these codes should not be under the control of the Subscriber, then the Subscriber must immediately change the codes, and if it is not possible, suspend the validity of the Certificates;

5.2.9 suspend the Certificates immediately if he/she has lost his/her SEB-card;

5.2.10 revoke the Certificates if he/she is unable to verify if his/her Private Keys were used during the time when the SEB-card was lost.

6 SK's Rights and Obligations

6.1 SK has the right to suspend SEB-card certificate 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 SK is obligated to:

6.2.1 supply 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 provide security with its internal security procedures;

6.2.4 accept applications for suspension of certificates 24 hours a day;

6.2.5 provide the possibility to check the validity of certificates 24 hours a day;

6.2.6 ensure that the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK;

6.2.7 ensure that the certification keys used in the supply of the certification service are activated on the basis of shared control;

6.2.8 suspend the validity or revoke Certificates upon the request of the Subscriber, SEB or on the grounds stipulated in applicable agreements set out in art. 9 or in law.

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 contains Certificate status information until the Certificate expires.

7.7 Additionally SK offers CRL service for checking Certificate status of SEB-card. 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 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 are included in the Certificates issued until 1 January 2017.

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 or revocation of Certificates. If the Subscriber finds his/her SEB-card and is certain that his/her Private Keys were not used during the suspension of the Certificates, the Subscriber may terminate suspension of the Certificates. In this case the Subscriber becomes solely and fully responsible for any consequences of Authentication and 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 the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK;

8.6.3 the certification keys used to provide the certification service are activated on the basis of shared control;

8.6.4 it has compulsory insurance contracts covering all SK services to ensure compensation for damages caused by SK's breach of obligations;

8.6.5 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.

8.7 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 the SEB card, 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, CRL and OCSP Profile for SEB-cards, 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 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 Authentication, the person conducting the identification is sent the Certificate that has been entered onto Subscriber´s SEB card and contains Subscriber´s 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 contains the Subscriber's 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 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.

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 SEB-card 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://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. The applications for revoking SEB-card certificates are accepted at SEB Customer Service Points or by sending an electronically signed application to personal@seb.ee.

14.3. SEB Customer Service Point contact information and operating hours are available in the SEB intranet.

14.4. The applications for suspension of SEB-card certificates are accepted 24/7 at (+372) 6655 100, at SEB Customer Service Point or at SK.