Terms and Conditions for Use of Organisation Certificates

Valid from 3 February 2017

1. Definitions and acronyms

Term/Acronym	Definition
CA	Certificate Authority
CP	Within the meaning of this Terms and Conditions the meaning of the term "CP" encompasses SK Certificate Policy for Organisation Certificates and SK Certificate Policy for TLS Server Certificates
CPS	SK Certification Practice Statement for Organisation Certificates
CRL	Certificate Revocation List
eIDAS	Regulation (EU) No 910/2014 of 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
HSM	Hardware Security Modules
OCSP	Online Certificate Status Protocol
Certificate	TLS Server Certificate, e-Seal Certificate, Certificate for Encryption, Certificate for Authentication. Within the meaning of these Terms and Conditions, the term "Certificate" encompasses all the previously listed certificates
Certificate Profile	Document that determines the profile and minimum requirements for the Certificate.
OID	Object identifier
Private Key	The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key
Public Key	The key pair that may be publicly disclosed by the holder of corresponding private key and that is used by Relying Party to verify digital 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 the eIDAS Regulation
Relying Party	Entity that relies upon the information contained within a certificate

Secure Cryptographic Device	Device that holds the user's Private Key, protects this key against compromise and performs signing or decryption functions on behalf of the user.
SK	AS Sertifitseerimiskeskus, a provider of certification services
Subscriber	Legal person bound by agreement with CA to any subscriber obligations
Terms and Conditions	Present document that describes the obligations and responsibilities of the Subscriber while using the Organisation certificates. The Subscriber must be familiar with the document and accept the terms and conditions described within when receiving the certificates

2. General terms

2.1. Present Terms and Conditions govern Subscribers' use of the Certificates and constitute a legally binding contract between Subscriber and SK.

2.2. The Terms and Conditions for use of Certificates and other applicable agreements are binding for the Subscriber for the entire term of validity of the Certificate and also after the revocation thereof in the event that legal consequences have been caused by activities performed with the formerly valid certificate and the term for contestation thereof has not expired.

2.3. SK issues Certificates to legal persons.

2.4. The Certificate is deemed accepted if within 14 (fourteen) days after the Terms and Conditions are signed, no complaints are made.

2.5. The Subscriber files an application for the requested certificate on SK's website at https://www.sk.ee/en/services/. The application is signed with an Advanced or Qualified Electronic Signature compliant with eIDAS by a legal person's representative or authorised person.

2.6. SK processes Certificate applications within 5 working days after receiving the respective application which includes all necessary data and is compliant with requirements of CPS.

2.7. SK does not issue Certificates to Subscribers that are bankrupt or in the process of liquidation and whose activities are suspended or in other similar state according to the legislation of its country of origin.

2.8. For issuance of e-Seal Certificates, the Subscriber must be registered in the Estonian Business Register or in Estonian Non-Profit Associations and Foundations Register or the Estonian Register of State and Local Government Organisations.

2.9. For issuance of TLS Server Certificates, Certificates for Encryption or Certificates for Authentication, the Subscriber must be registered in the Estonian, Latvian, Lithuanian, Finnish or Swedish Business Register and can be found from the European Business Register or in Estonian Non-Profit Associations and Foundations Register or the Estonian Register of State and Local Government Organisations.

2.10. SK has the right to refuse to issue a Certificate on the basis of CP and CPS. The Subscriber is notified of the acceptance or rejection of the Certificate application.

2.11. SK has the right to amend the Terms and Conditions at any time should SK have a justified need for such amendments. The amended Terms and Conditions along with the effective date, which cannot be earlier than 90 days after publication, are published electronically on the website of SK at https://www.sk.ee/en/repository/conditions-for-use-of-certificates/. Within 30 days of amendment publication, the Subscriber has the chance to provide reasoned comments followed by a period of up to 30 days for comment analysis by SK. 60 days after the amendment publication, the new version of Terms and Conditions is published electronically on SK's website, otherwise the amendment is withdrawn.

2.12. In case of changes in compliance requirements, SK has the right to amend Terms and Conditions along with the enforcement date, which cannot be earlier than 30 days after publication. The amended Terms and Conditions are published electronically on SK's website at https://www.sk.ee/en/repository/conditions-for-use-of-certificates/.

3. Certificate type, validation procedures and usage

3.1. These Terms and Conditions are applicable to following certificate types:

Certificate type	Usage	Certification policy applied and published	OID	Summary
TLS Server Certificate	Certificate issued to TLS server (HTTPS, IMAPS, FTPS, etc.) for proof of authenticity of TLS server owner	AS Sertifitseerimiskeskus – Certificate Policy for TLS Server Certificates, published: https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.7.2.	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(7.2)
		ETSI EN 319 411-1 Policy: OVCP	0.4.0.2024.1.7	itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)
		CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")	2.23.140.1.2.2	{joint-iso-itu-t(2) internationa l-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-v alidated(2)} (2.23.140.1.2.2)
e-Seal Certificate	Certificate used for proof of integrity of a digital document and the relation with the owner of such document	AS Sertifitseerimiskeskus - Certificate Policy for Organisation Certificates, published: https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.7.3	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(7.3)
		ETSI EN 319 411-2 Policy: QCP-l	0.4.0.194112.1.1.	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) itu-t(0) identified-organization(4)

				etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)
e-Seal Certificate on QSCD	Certificate used for proof of integrity of a digital document and the relation with the owner of such document	AS Sertifitseerimiskeskus - Certificate Policy for Organisation Certificates, published: https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.7.3	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(7.3)
		ETSI EN 319 411-2 Policy: QCP-l-qscd	0.4.0.194112.1.3	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)
Certificates for Encryption	Certificate used for data encryption	AS Sertifitseerimiskeskus - Certificate Policy for Organisation Certificates, published: https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.7.3	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(7.3)
		ETSI EN 319 411-1 Policy: NCP	0.4.0.2042.1.1	itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)
Certificates for Authentication	Certificate used for authentication of the Subscriber in WWW, S/MIME or other data processing systems.	AS Sertifitseerimiskeskus - Certificate Policy for Organisation Certificates, published: https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.7.3	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(7.3)
		ETSI EN 319 411-1 Policy: NCP	0.4.0.2042.1.1	itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)

3.2. Various areas of application can be combined into a single Certificate. The e-Seal Certificate cannot be combined with other areas of application.

3.3. The use of the Certificates is prohibited for any of the following purposes:

3.3.1. unlawful activity (including cyber attacks and attempts to damage the Certificate);

3.3.2. issuance of new Certificates and information on Certificate validity;

3.3.3. use of the e-Seal Certificate for signing documents which can bring about unwanted consequences (including signing such documents during testing of the systems).

4. Reliance limits

4.1. 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.

4.2. The expected lifetime of the Certificate is specified in the Certificate.

5. Subscriber’s rights and obligations

5.1. The Subscriber is obligated to:

5.1.1. use the Certificates in compliance with the Terms and Conditions, including applicable agreements set out in art. 9, and the laws of the Republic of Estonia and European Union;

5.1.2. use its Private Key in accordance with the Terms and Conditions and CPS;

5.1.3. ensure that Subscriber's Private Key is used under its control;

5.1.4. back up and archive its Private Key;

5.1.5. create e-Seals only by using the QSCD or Secure Cryptographic Device;

5.1.6. in case of suspension and revocation application, ascertain on the basis of LDAP directory or CRL that the Certificate has been suspended or revoked;

5.1.7. supply true and adequate information in the application for the services;

5.1.8. not use the Private Key in case of compromise;

5.1.9. inform about any changes in the data submitted by the Subscriber, including the following:

5.1.9.1. changes in the contact persons;

5.1.9.2. beginning of bankruptcy, liquidation, suspension of operations or other similar state according to the legislation of its country of origin;

5.1.9.3. changes in name and/or IP addresses of the server or device;

5.1.9.4. any changes in the Certificate data;

5.1.9.5. withdrawal of Common Criteria Certificate issued for QSCD;

5.1.9.6. replacement of QSCD or its firmware.

5.1.10. file an application for revocation, in case the Subscriber does not have the ability to submit an application for termination of suspension.

5.2. In case the e-Seal Certificate Subscriber keys are generated by the Subscriber on QSCD, the Subscriber has responsibility for ensuring that the device is compliant throughout the validity period of the Certificate and that the Private Key cannot be copied or extracted from the device.

5.3. If the QSCD is replaced, SK asks for proof that the Subscriber has performed the transfer of keys in a properly secured way. If the Subscriber is unable to present the necessary information, SK will revoke the Certificate.

5.4. In the event that the Subscriber has lost possession of the Private Key of a Certificate or there is a danger of such event occurring, the Subscriber must immediately submit an application to SK for suspension (only in case of e-Seals) or revocation of the Certificate issued to the Subscriber as set out in 14.2.

5.5. The Subscriber is not responsible for the acts performed during the suspension of Certificate. In case the Subscriber terminates the suspension of the Certificate, the Subscriber will be solely and fully responsible for any consequences arising from transactions using the Certificate during the time when the Certificate was suspended. If the Subscriber has a suspicion that the Private Key has gone out of control of the Subscriber at the time of suspension of Certificate, the Subscriber is obliged to revoke the Certificate.

6.SK's rights and obligations

6.1. SK has the right to refuse to provide the service if the Subscriber has intentionally presented false, incorrect or incomplete information in the application for the service;

6.2. In case the data on an application for the Certificate is missing, contains grammatical errors, contradicts with the Certificate Profile or the data in registries, then without notifying the Subscriber, SK can change the information according to CPS.

6.3. In case SK is not certain that the device used by the Subscriber is QSCD, SK issues e-Seal Certificate on Secure Cryptographic Device.

6.4. SK has the right to revoke any Certificate if one or more of the following occurs:

6.4.1. the Subscriber requests in writing that SK revoke the Certificate;

6.4.2. the Subscriber notifies SK that the original Certificate request was not authorised and does not retroactively grant authorisation;

6.4.3. SK obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements;

6.4.4. SK obtains evidence that the Certificate was misused;

6.4.5. SK is made aware that a Subscriber has violated one or more of its obligations under the Terms and Conditions;

6.4.6. the owner of a Certificate has not paid for the issued Certificate within the determined period of time;

6.4.7. SK is made aware of a material change in the information contained in the Certificate;

6.4.8. SK is made aware that the Certificate was not issued in accordance with the CPS and/or CP;

6.4.9. SK determines that any of the information appearing in the Certificate is inaccurate or misleading;

6.4.10. SK ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

6.4.11. SK's right to issue Certificates is revoked or terminated, unless SK has made arrangements to continue maintaining the CRL/OCSP repository;

6.4.12. SK is made aware of a possible compromise of the Private Key of the SK CA used for issuing the Certificate;

6.4.13. revocation is required by the CP;

6.4.14. the technical content or format of the Certificate presents an unacceptable risk to Relying Parties;

6.4.15. in case of Certificate modification the erroneous Certificate will be revoked.

6.5. SK has the right to revoke TLS Certificates in case SK is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant

licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name).

6.6. SK has the right to revoke e-Seal Certificates in case SK is made aware that the e-Seal on QSCD Private Key is no longer in a hardware module that is compliant with QSCD requirements.

6.7. SK immediately informs the Subscriber of suspension (only in case of e-Seal Certificates) or revocation of the validity of a Certificate. In the event that the validity of a Certificate was not suspended or revoked by the Subscriber of a Certificate, the message shall be communicated to the e-mail address of the contact person of the Subscriber.

7. Certificate status checking obligations of relying parties

7.1. A 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 CP.

7.2. SK offers CRL and OCSP services for checking certificate status. Services are accessible over HTTP protocol. 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 1 July 2016.

7.3. 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.

7.4. CRL checking availability

7.4.1. If a Relying Party checks Certificate validity against the CRL, the party must use the latest versions of the CRL for the purpose. The CRL contains the revoked Certificates, the date and reasons for revocation.

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

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

7.4.4. Relying Party uses CRL service on its own responsibility.

7.5. OCSP checking availability

7.5.1. The OCSP service is free of charge and publicly accessible at https://aia.sk.ee/klass3-2010.

7.5.2. For other methods of Certificate status disclosure, SK may set a fee in the price list or require a corresponding agreement.

8. Limited warranty and disclaimer/Limitation of liability

8.1. The Subscriber ensures that it:

8.1.1. is solely responsible for the use of its Private Key and Certificate.

8.1.2. is aware that activities performed on the basis of an expired and/or revoked Certificate are void.

8.2. SK ensures that:

8.2.1. the certification service is provided in accordance with CPS, CP and the relevant legislation of the Republic of Estonia and European Union;

8.2.2. it accepts applications for suspension of e-Seal Certificates 24 hours a day;

8.2.3. it accepts applications for termination 24 hours a day;

8.2.4. Certificates are revoked immediately after the request's legality has been verified, but no later than 12 hours after an application for revocation has been submitted. 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.

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

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

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

8.2.8. 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.

8.3. SK is not liable for:

8.3.1. 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;

8.3.2. 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;

8.3.3. 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. AS Sertifitseerimiskeskus – Certificate Policy for Organisation Certificates, published at https://sk.ee/en/repository/CP/;

9.1.2. AS Sertifitseerimiskeskus – Certificate Policy for TLS Server Certificates, published at https://sk.ee/en/repository/CP/;

9.1.3. AS Sertifitseerimiskeskus – Certification Practice Statement for KLASS3-SK 2010, published at https://sk.ee/en/repository/CPS/;

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

9.1.5. Certificate, CRL and OCSP Profile for Organisation Certificates Issued by SK, published at: https://sk.ee/en/repository/profiles/

9.1.6. 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/, when handling personal information and logging information.

10.2. The Subscriber is aware and approves of the fact that its name and registry code are published in the list of valid Certificates.

10.3. The Subscriber gives its consent that its Certificate is published and available for retrieval.

10.4. The Subscriber is aware that by using Certificates for verifying the integrity of a digital document, the Certificate containing its name and registry code shall be attached to the digitally verified document.

10.5. 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.

10.6. 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.

10.7. Disclosure or forwarding of confidential information to a third party is permitted only with the written consent of the legal possessor of the information on the basis of a court order or in other cases provided by law.

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

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

11. Refund policy

11.1. The Subscriber has the right to request refund in the form of modification of the Certificate within 14 days after initial issuance of the Certificate.
11.2. SK handles refund requests 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 licenses, trust marks, and audit

13.1. The certification service for e-Seal Certificates is registered in the Estonian Trusted List 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, 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 and Customer Service Point:
AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu mnt. 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 are accepted 24/7 at:
Phone +372 610 1880
E-mail: revoke@sk.ee

14.3. The most recent information on the Customer Service Point and its contact details is available at SK's website: https://sk.ee/en/kontakt/.