Terms and Conditions for Use of Organisation Certificates

Draft version published 01.04.2016

Valid from 01.07.2016

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 this Terms and Conditions, the term "Certificate" encompasses all the previously listed certificates
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 eIDAS regulation
Relying Party	Entity that relies upon either the information contained within a certificate
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 for the Subscriber while using the Organisation certificates. The Subscriber has to 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. 14 (fourteen) days after signing the Terms and Conditions, if no complains are raised, are deemed acceptance of the Certificate.

2.5. The Subscriber files an application for the requested certificate on SK-s homepage at https://www.sk.ee/en/services/. The application is signed with an Advanced or Qualified Electronic Signature compliant to eIDAS by 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 the Certificate to Subscriber, that is bankrupted or in the process of liquidation and its activities are suspended or in other similar state in terms of legislation of its country of origin.

2.8. For issuing e-Seal Certificate, the Subscriber has to 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 issuing TLS Server Certificate, Certificates for Encryption or Certificates for Authentication, the Subscriber has to 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 bases of CPS. The Subscriber is notified of acceptance or rejection of the certificate application.

2.11. SK has the right to amend Terms and Conditions at any time should SK have a justified need for such amendments. The amended Terms and Conditions along with the enforcement date, which cannot be earlier than 90 days after publication, is published electronically on the website of SK website at 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 maximum 30-day period for comment analysis by SK. 60 days after the amendment publication, the new version of Terms and Conditions is published electronically on SK's web page, otherwise the amendment is withdrawn.

3. Certificates type, validation procedures and usage

3.1. This 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-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 can not 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 attempt to infringe the certificate);

3.3.2. issuance of new certificates and information on certificate validity;

3.3.3. using 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 about certificate applications, registration information and requests or applications for suspension, termination of suspension and revocation are retained at least for 10 years after validity of relevant certificate.

4.2. Expected lifetime of Certificate is specified in 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 Terms and Conditions and CPS;

5.1.3. ensure that Subscribers´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 QSCD device;

5.1.6. in case of suspension and revocation application, to 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. inform about any changes in the data submitted by the Subscriber, including following:

5.1.8.1. changes in the contact persons;

5.1.8.2. beginning of bankruptcy, liquidation, suspension of operations or other similar state in terms of legislation of its country of origin;

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

5.1.8.4. any changes in the Certificate data;

5.1.8.5. withdrawal of Common Criteria Certificate issued for QSCD;

5.1.8.6. replacement of QSCD or its firmware.

5.1.9. In case the Subscriber keys of e-Seal Certificate are generated by the Subscriber in a hardware module (HSM, Smartcard or other cryptographic token) that is compliant to requirements of 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.

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

5.1.11. In the event that the Subscriber has lost possession of the Private key of a Certificate or there is a danger of the aforesaid event, the Subscriber submits immediately 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 14.3.

5.1.12. The Subscriber is not responsible for the acts performed during the suspension of Certificate. In case the Subscriber will terminate the suspension of Certificate, the Subscriber will be solely and fully responsible for any consequences arising from transactions using the Certificate during the time when the Certificate were 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. SK has the right to revoke any Certificate, if one or more of the following occurs:

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

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

6.2.3. 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;

6.2.4. SK obtains evidence that the Certificate was misused;

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

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

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

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

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

6.2.10. SK ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
6.2.11. SK's right to issue Certificates is revoked or terminated, unless the SK has made arrangements to continue maintaining the CRL/OCSP repository;
6.2.12. SK is made aware of a possible compromise of the Private Key of the SK CA used for issuing the Certificate;
6.2.13. revocation is required by the CP;
6.2.14. the technical content or format of the Certificate presents an unacceptable risk to Relying Parties;
6.2.15. In case of Certificate modification the erroneous Certificate will be revoked.

6.3. SK has the right to revoke TLS Certificate, 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).

6.4. SK has the right to revoke e-Seal Certificate, in case SK is made aware that Private Key of e-Seal is no longer in a hardware module that is compliant to requirements of QSCD.

6.5. 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. 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. SK offers CRL and OCSP services for checking certificate status. Services are accessible using HTTP protocol. The URL-s 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.

7.3. SK ensures Certificate Status Services availability 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 Relying Party checks the 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 when these were revoked and the reason for that.

7.4.2. A valid CRL is free of charge and is 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 issuance of CRL.

7.5. OCSP cheking availabilty

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

7.5.2. In case of other manners of publication information on status of the Certificate, SK may fix a fee in a price list or require corresponding agreement.

8. Limited warranty and disclaimer/Limitation of liability

8.1. The Subscriber ensures that:

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 supply of the Certification service is in accordance with CPS, CP and the relevant legislation of the Republic of Estonia and European Union;

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

8.2.3. accepts application for termination of 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 in the supply of the certification service are activated on the basis of shared control;

8.2.7. has compulsory insurance contracts, which cover all SK services to ensure compensation for damage which is caused as a result of violation of the obligations of SK;

8.2.8. informs all Subscribers before SK terminates service of Certificates and maintains the documentation related to the terminated service of Certificates and information needed according process set out in CPS.

8.3. SK is not liable for:

8.3.1. the secrecy of the Private Keys of the Subscribers, possible misuse of the certificates or inadequate checks of the Certificates or for the wrong decisions of a Relying Party or any consequences due to errors 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. non-fulfilment if such non-fulfilment 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 https://sk.ee/en/repository/CP/;

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

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

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

9.1.5. Certificate, CRL and OCSP Profile for Organisation Certificates Issued by SK, published: 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 Principles of Client Data Protection 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 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.

10.4. All information that has become known while providing services and that is not intended for publication (e.g. information that had been known to SK because of operating and providing Trust Services) is confidential. Subscriber has a right to get information from SK about him/herself according to legal acts.
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. 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.
10.7. 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 has the right for fixing errors in certificate within 14 days after initial issuance of 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 and 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 compliant 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 request should be directed to Contact info given 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. Prerequisite requirement of this registration is compliance with applicable regulations and standards.

13.2. Conformity assessment body is accredited in accordance with Regulation EC no 765/2008 as competent to carry out conformity assessment of qualifed 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 info

14.1. Trust Service Provider and Customer Service Point:
AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu Ave. 141, 11314
Tallinn, ESTONIA
(Mon-Fri 9.00-18.00 East 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 Customer Service Point and its contact is available at SK's website: https://sk.ee/en/kontakt/.