Terms and Conditions for Use of Certificates of non-qualified Smart-ID

Valid from 01.01.2017

Definitions and Acronyms

Term	Definition
Advanced Electronic Signature	Electronic Signature which meets the requirements provided in Article 26 of eIDAS.
Authentication	Unique identification of a person by checking his/her alleged identity.
Authentication Certificate	Certificate is intended for Authentication.
AS Sertifitseerimiskeskus Trust Services Practice Statement (SK PS)	A statement of practices that SK employs in providing Trust Services.
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 with its electronic signature.
Certificate Policy (CP)	Certificate Policy for non-qualified Smart-ID.
Certificate Profile	Certificate and OCSP profile for Smart-ID.
Certification Practice Statement (CPS)	AS Sertifitseerimiskeskus - NQ-SK Certification Practice Statement.
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.
Identity Provider	An organisation who is providing electronic authentication means and who is responsible for creating electronic identities which are used for issuing NQ Smart-ID Certificates. Identity Provider has been verified by Smart-ID Provider to follow the Requirements for Identity Providers for non-qualified certificates.
non-qualified Electronic Signature Certificate	An electronic attestation which links electronic signature validation data to a natural person and confirms at least the name of that person.
NQ Smart-ID	Smart-ID which contains one pair of Certificates consisting of the Authentication Certificate and the non-qualified Electronic Signature Certificate and their corresponding Private Keys.
Object Identifier	An identifier used to uniquely name an object (OID).
OCSP	Online Certificate Status Protocol.
PIN code	Activation code for the Private Key that corresponds to Authentication Certificate and for the Private Key that corresponds to the 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.
Relying Party	Entity that relies on the information contained within a Certificate.

SK	AS Sertifitseerimiskeskus, a provider of certification service.
SK PS	AS Sertifitseerimiskeskus Trust Services Practice Statement.
SLA	Service Level Agreement.
Smart-ID	Smart-ID is the new generation electronic ID which provides the Subscriber with means for Electronic Authentication and Electronic Signature.
Smart-ID Account	Subscriber has to register a Smart-ID Account to use services provided by the Smart-ID System. Smart-ID Account binds Smart-ID Application instance to a Subscriber's identity in the Smart-ID System. In the course of Smart-ID Account creation and registration, the identity of the Smart-ID Account owner (Subscriber) is proofed by a Registration Authority and the relation between the identity and a key pair is certified by a Certificate Authority. Smart-ID Account has an Advanced Electronic Signature key and an Authentication key.
Smart-ID Provider	An organisation that is legally responsible for the Smart-ID system. SK is the Smart-ID provider.
Smart-ID Application	A technical component of the Smart-ID system. A Smart-ID Application installed on a Subscriber's Mobile Device that provides access to non-qualified Smart-ID service.
Smart-ID System	A technical and organisational environment which enables Electronic Authentication and Electronic Signatures in an electronic environment. The Smart-ID system provides services that allow Subscribers (Smart-ID Account owners) to authenticate themselves to services, to give Electronic Signatures, and to manage their Smart-ID Accounts.
Subscriber	A natural person to whom the NQ Smart-ID Certificates are issued.
Terms and Conditions	Document that describes obligations and responsibilities of the Subscriber with respect to using Certificates. The Subscriber has to be familiar with the document and accept the Terms and Conditions upon receipt of 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 NQ Smart-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 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 on the website https://sk.ee/en.

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

2 **Certificate Acceptance**

2.1 The Subscriber confirms NQ Smart-ID Certificate issuance in Smart-ID Application. Corresponding confirmation is deemed Certificate acceptance for NQ Smart-ID.

2.2 If the Certificate re-key is performed the Subscriber confirms Certificate issuance in Smart-ID Application.

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

Certificate Type	Usage	Certification Policy Applied and Published	OID	Summary
Certificates for Smart-ID	Certificate for Electronic Signature is intended for: creating Advanced Electronic Signatures compliant with eIDAS.	AS Sertifitseerimiskeskus – Certificate Policy for non-qualified Smart-ID, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.17.1	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(17.1)
		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)
	Authentication Certificate is intended for: authentication.	AS Sertifitseerimiskeskus – Certificate Policy for non-qualified Smart-ID, published https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.17.1	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(17.1)
		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)

3.1 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 of the NQ Smart-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 Advanced 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 NQ Smart-ID.

5.2 The Subscriber is obligated to:

5.2.1 accept the Terms and Conditions;
5.2.2 adhere to the requirements provided by SK;
5.2.3 use his/her Private Key and Certificate in accordance with the Terms and Conditions, including applicable agreements set out in art. 9, and the laws of the Republic of Estonia and European Union;
5.2.4 ensure that Subscribers´s Private Key is used under his/her control;
5.2.5 present true and correct information to Smart-ID System;
5.2.6 notify Smart-ID Provider of the correct details during a reasonable time in case of a change in his/her personal details;
5.2.7 immediately inform SK of a possibility of unauthorised use of his/her Private Key and revokes his/her Certificates;
5.2.8 immediately revoke his/her Certificates if his/her Private Key has gone out of his/her possession;
5.2.9 he/she immediately revokes his/her certificates or applies for new NQ Smart-ID if his/her PIN codes have gone out of his/her control.

6 SK's Rights and Obligations

6.1 SK is entitled to revoke all Certificates issued for identities provided by Identity Provider if SK has withdrawn Identity Provider status from the corresponding Identity Provider.

6.2 SK is obligated to:

6.3 supply certification service in accordance with the applicable agreements set out in art 9 and relevant legislation;

6.4 keep account of the certificates issued by it and of their validity;

6.5 provide security with its internal security procedures;

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

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

6.8 provide the certification keys used in the supply of the certification service are activated on the basis of shared control.

7 Certificate Status Checking Obligations of Relying Parties

7.1 A Relying Party 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 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 an 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 A Relying Party validates the identity from NQ Smart-ID Certificate against personal information known by Relying Party on first authentication of this Subscriber to it's system.

7.5 A Relying Party is obliged:

7.5.1 not to create any new identities relying solely on the information from NQ Smart-ID Certificates;
7.5.2 to start changing the Subscriber's name in its database if the name in the Certificate and Identity Provider's database does not match.

7.6 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.

7.7 SK offers OCSP service for checking Certificate status. Service is accessible over HTTP protocol.

7.8 A Relying Party verifies the validity of the Certificate by checking Certificates validity against OCSP. SK offers OCSP with following checking availability:

7.8.1 An OCSP service is free of charge and publicly accessible at http://aia.sk.ee/nq2016;
7.8.2 SK offers an OCSP service with better SLA under agreement and price list;
7.8.3 The URL of the OCSP service is included in the certificate on the Authority Information Access (AIA) field in accordance with the Certificate Profile.

8 Obligations of Other Participants

8.1 Smart-ID Provider ensures that:

8.1.1 it adheres to the key generation and storage procedures under its control and described in the CPS;
8.1.2 it adheres to provisions of fees described in the CPS;
8.1.3 it transfers the correct Certificate and correct Certificate status information;
8.1.4 before giving out Identity Provider status to an entity, the identity quality level of that entity is evaluated by verifying that the entity follows Requirements for Identity Providers for non-qualified certificates.

8.2 Smart-ID Provider is entitled to withdraw Identity Provider status if it obtains evidence that Requirements for Identity Providers for non-qualified certificates are not followed by Identity Provider.

8.3 Identity Provider ensures compliance with the Requirements for Identity Providers for non-qualified certificates.

9 Limited Warranty and Disclaimer/Limitation of Liability

9.1 The Subscriber is solely responsible for the maintenance of his/her Private Key.

9.2 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.

9.3 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.

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

9.5 SK ensures that:

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

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

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

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

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

9.6 SK is not financially liable for the information contained in NQ Smart-ID Certificates.

9.7 SK is not liable for:

9.7.1 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;

9.7.2 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, or any other public authority;

9.7.3 the failure to perform if such failure is occasioned by force majeure.

10 Applicable Agreements, CPS, CP

10.1 Relevant agreements, policies and practice statements related to Terms and Conditions for use of Certificates are:

10.1.1 AS Sertifitseerimiskeskus – Certificate Policy for non-qualified Smart-ID, published at https://sk.ee/en/repository/CP/;

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

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

10.1.4 Certificate and OCSP Profile for Smart-ID, published at: https://www.sk.ee/en/repository/profiles/;

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

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

11 Privacy Policy and Confidentiality

11.1 SK follows the Principles of Client Data Protection, provided in SK repository https://sk.ee/en/repository/data-protection/ and other legal acts of Estonian Republic, when handling personal information and logging information.

11.2 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 in Subscriber´s document and contains Subscriber´s name and personal identification code.

11.3 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.

11.4 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.

11.5 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.

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

12 Refund Policy

12.1 SK handles refund case-by-case.

13 Applicable law, complaints and dispute resolution

13.1 The certification service is governed by the jurisdictions of Estonia and European Union as the location where SK is registered as a CA.

13.2 The certification service for NQ Smart-ID complies with the requirements of Trust Services as described in eIDAS.

13.3 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.

13.4 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.

13.5 The Subscriber or other party can submit their claim or complaint on the following email: info@sk.ee.

13.6 All dispute requests should be sent to contact information provided in these Terms and Conditions.

14 Contact Information

14.1 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

14.2. The applications for revoking NQ Smart-ID certificates are accepted via 24/7 Help Line: 9001807 or 1807 and/or self-service web portal and/or Smart-ID Application and/or Customer Service Points.

14.3. Information and contact details of the Help Line and self-service web portal and Customer Service Points is available on SK's website https://www.sk.ee/en.