Terms and Conditions for Use of Certificates for ID-1 Format Identity Documents of the Republic of Estonia

Valid from 12.05.2021

Definitions and Acronyms

Term/Acronym	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
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	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card.
CPS	SK ID Solutions AS – ESTEID2018 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 or Diplomatic-ID).
Digi-ID	Digital identity card for Estonian resident and digital identity card for e-resident. Within the meaning of the Terms and Conditions, the term "Digi-ID" encompasses the previously listed identity documents.
Diplomatic-ID	Diplomatic identity card
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.
IDA	Identity Documents Act.
ID-card	Identity card for Estonian citizen, identity card for European Union citizen, residence permit card for long-term resident and residence permit card for temporary residence citizen. Within the meaning of the Terms and Conditions, the term "ID-card" encompasses all the previously listed identity documents.
MFA	Ministry of Foreign Affairs.
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.
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.
Qualified Certificate	A certificate for electronic signatures, that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of eIDAS Regulation.
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.
Relying Party	Entity that relies on the information contained within a Certificate.
Secure Cryptographic Device	Device which holds the Private Key of the user, protects this key against compromise and performs signing or decryption functions on behalf of the user.
SK	SK ID Solutions AS.
SK PS	SK ID Solutions AS Trust Services Practice Statement.
SLA	Service Level Agreement.
Subscriber	A natural person to whom the Certificates of ID-card, Digi-ID or Diplomatic-ID are issued as a public service if he/she has a statutory right and has requested it.
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, 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 applying for 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://www.skidsolutions.eu/en.
1.5. SK issues Certificates to natural persons or to natural person's representative entitled by IDA.

2. Certificate Acceptance

2.1. In case of ID-card, Digi-ID or Diplomatic-ID Certificates issuance:

2.1.1. signing the file of the ID-card, Digi-ID or Diplomatic-ID issuance as well as confirmation that the ID-card, Digi-ID or Diplomatic-ID has been handed over to the Subscriber are deemed Certificate acceptance.

3. Certificate Type, Validation Procedures and Usage

Certificate Type	Usage	Certification Policy Applied and Published	OID	Summary
Certificates for ID-card of Estonian citizen	Qualified Electronic Signature Certificate is intended for:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.51361.1.1	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.1).
	creating Qualified Electronic Signatures compliant with eIDAS	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:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.1	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.1).
	Authentication, Encryption, secure e-mail	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 ID-card of European Union citizen	Qualified Electronic Signature Certificate is intended for:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.2	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.2).
	creating Qualified Electronic Signatures compliant with eIDAS	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:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.2	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.2).

	Authentication, Encryption, secure e-mail	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:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.51361.1.1.3	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.3).
	creating Qualified Electronic Signatures compliant with eIDAS	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:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.51361.1.1.3	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.3).
	Authentication, Encryption, secure e-mail	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 of e-Resident	Qualified Electronic Signature Certificate is intended for:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.4	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.4).
	creating Qualified Electronic Signatures compliant with eIDAS	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:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.4	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.4).
	Authentication, Encryption, secure e-mail	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 residence card of long-term resident	Qualified Electronic Signature Certificate is intended for:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.5	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.5).

	creating Qualified Electronic Signatures compliant with eIDAS	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:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.5	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.5).
	Authentication, Encryption, secure e-mail	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 residence card of temporary resident citizen	Qualified Electronic Signature Certificate is intended for:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published www.id.eehttps://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.6	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.6).
	creating Qualified Electronic Signatures compliant with eIDAS	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:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.6	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.6).
	Authentication, Encryption, secure e-mail	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 residence card of family members of citizen of European Union	Qualified Electronic Signature Certificate is intended for:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.7	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.7).
	creating Qualified Electronic Signatures compliant with eIDAS	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:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.5136 1.1.7	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) PBGB attribute in IANA register (51361) Certification service attribute (1.7).

	Authentication, Encryption, secure e-mail	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 Diplomatic-ID	Qualified Electronic Signature Certificate is intended for:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.51455.1.1	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) MFA attribute in IANA register (51455) Certification service attribute (1.1).
	creating Qualified Electronic Signatures compliant with eIDAS	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:	Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published https://www.id.ee/?lang=en&id=30500	1.3.6.1.4.1.51455.1.1	internet attribute (1.3.6.1) private entity attribute (4) registered business attribute given by private business manager IANA (1) MFA attribute in IANA register (51455) Certification service attribute (1.1).
	Authentication, Encryption, secure e-mail	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 or Diplomatic-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 suspended or 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 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 Keys and Certificates solely on a secure cryptographic device handed over to him/her at Customer Service Point of PBGB or MFA;

5.2.5. use his/her Private Keys and Certificates 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;

5.2.6. 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;

5.2.7. ensure that Subscriber´s Private Key is used under its control.

5.3. The Subscriber is aware that SK publishes his/her valid Certificates during their validity period via LDAP directory service.

5.4. The Subscriber is obligated to present true and correct information to PBGB while presenting an application for ID-card or Digi-ID.

5.5. The Subscriber is obligated to present true and correct information to MFA while presenting an application for Diplomatic-ID.

5.6. In case of a change in personal details, the Subscriber is obligated to immediately notify PBGB or MFA of the correct details in accordance with the established legislation.

5.7. The 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 by submitting a signed application at PBGB Customer Service Point. Suspended Certificates can be reactivated and new PIN codes can be applied;

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 signed application submitted to PBGB Customer Service Point.

5.8. The Subscriber´s obligations in case of the loss or unauthorised use of Diplomatic-ID:

5.8.1. having discovered the loss of Diplomatic-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 by submitting a signed application at MFA Customer Service Point. Suspended Certificates can be reactivated and new PIN codes can be applied;

5.8.2. if the Subscriber has a suspicion that Diplomatic-ID has gone out of control of the Subscriber at the time of suspension of the Certificates, the Subscriber is obliged to revoke the Certificates;

5.8.3. certificates can be revoked only on the basis of a signed application submitted to MFA Customer Service Point.

5.9. Upon loss or theft of the ID-card, Digi-ID or Diplomatic-ID or it becoming unusable due to another reason, the Subscriber is obligated to immediately address the issue to the service of PBGB or MFA respectively for the ID-card, Digi-ID or Diplomatic-ID 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 Private Key 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 or Diplomatic-ID SK is obligated to:

6.2.1. supply the 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. accept applications for suspension of Certificates 24 hours a day;

6.2.4. provide the possibility to check the validity of Certificates on its website 24 hours a day;

6.2.5. provide security with its internal security procedures;

6.2.6. suspend or revoke a Certificate if requested by the Subscriber, PBGB or MFA or under any other circumstances specified in laws or legal acts;

6.2.7. inform the Subscriber by using @eesti.ee e-mail address and Subscriber's contact email address in the Certificate application, or only one of the mentioned email addresses, that their Certificate has been suspended, suspension has been terminated or Certificate has been revoked.

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 down-time 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 Certificate validity against OCSP. SK offers OCSP with following checking availability:

7.6.1. OCSP service is free of charge and publicly accessible at location provided in Certificate's Authority Information Access extension;

7.6.2. SK offers an OCSP service with better SLA under agreement and price list;

7.6.3. the URLs of the service is included in the Certificates on the Authority Information Access (AIA) field in accordance with the Certificate Profile;

7.6.4. OCSP contains Certificate status information until the Certificate expires.

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 shall check 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.skidsolutions.eu/en/repository/CRL/;

7.7.5. relying Party shall use CRL service on its own responsibility.

7.8. Revocation status information of the expired Certificate can be requested at the email address info@skidsolutions.eu.

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 Qualified 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 Qualified 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 ID-card, Digi-ID or Diplomatic-ID 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. 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. Police and Border Guard Board – Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published at: https://www.id.ee/?lang=en&id=30500;

9.1.2. SK ID Solutions AS – ESTEID2018 Certification Practice Statement, published at: https://www.skidsolutions.eu/en/repository/CPS/;

9.1.3. SK ID Solutions AS Trust Services Practice Statement, published at: https://www.skidsolutions.eu/en/repository/sk-ps/;

9.1.4. Certificate, CRL and OCSP Profile for ID-1 Format Identity Documents Issued by the Republic of Estonia, published at: https://www.skidsolutions.eu/en/repository/profiles/;

9.1.5. Principles of Processing Personal Data, published at: https://www.skidsolutions.eu/en/repository/data-protection/;

9.2. Current versions of all applicable documents are publicly available in SK repository: https://www.skidsolutions.eu/en/repository/.

10. Privacy Policy and Confidentiality

10.1. SK follows the Principles of Processing Personal Data, provided in SK repository https://www.skidsolutions.eu/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 Authentication is sent the Certificate that has been entered in the Subscriber´s Document and contains the 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 has been entered in their Document and contains their 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 has become 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. SK is entitled to perform checks from reliable sources related to the Subscriber's identity validation should SK consider it necessary for providing certification service.

10.8. 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 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@skidsolutions.eu.

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 Diplomatic-ID 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.skidsolutions.eu/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)

https://www.skidsolutions.eu/en

Phone +372 610 1880

Fax +372 610 1881

E-mail: info@skidsolutions.eu.

14.2. Suspension requests of ID-card, Digi-ID or Diplomatic-ID Certificates are accepted 24/7 at +1777 (or +372 677 3377).

14.3. Suspension requests of ID-card or Digi-ID Certificates are also accepted at PBGB Customer Service Point and suspension requests of Diplomatic-ID Certificates are also accepted at MFA Customer Service Point.

14.4. Revocation requests of ID-card or Digi-ID Certificates are accepted at PBGB Customer Service Point and revocation requests of Diplomatic-ID Certificates are accepted at MFA Customer Service Point.

14.5. User support for solving problems related to ID-card and Digi-ID usage can also be requested at (+ 372) 666 8888.

14.6. The list and operating hours of PBGB and MFA Customer Service Points can be checked on the websites of PBGB, MFA and SK: https://www.politsei.ee/en/services/services,

http://www.vm.ee/en/country-representations/estonian-representations and
https://www.skidsolutions.eu/en/kontakt/customerservice/.