Document Information	
Name	SK ID Solutions AS - Certificate Policy for Digi-ID
Version number	11.0
Version No. and date	Changes
10.04.2020 11.0	Clause 1.3.5 - added that Card Manufacturer is no longer responsible for preparing the cards and providing technical environment for personalisation in the RA office; Clause 1.5.4 - added that SK performs annual review of this CP.
03.07.2019 10.0	Please note: Certificate re-key to extend the validity of the digital identity document and of the e-residence card was performed according to the current Certificate Policy until 30th April 2019. The provisions that describe the requirements for validity extension, such as provisions on Certificate Re-Key for validity extension are no longer applicable. However, the corresponding requirements have been left in this Certificate Policy to facilitate understanding how validity extension of the digital identity document and of the e-residence card was performed.
01.05.2019 9.0	Please note: Qualified Electronic Signature and Authentication Certificates for Estonian digital identity document and for the e-residence card were issued according to the current Certificate Policy until December 2018. The provisions that describe requirements for issuance of the Certificates, such as provisions on identification, certificate application and key pair generation and installation are no longer applicable. However, the requirements on the issuance of Qualified Electronic Signature and Authentication Certificates have been left in this Certificate Policy to facilitate understanding how issuance of the Certificates for Estonian digital identity document and for the e-residence card was performed. Certificate re-key to extend the validity of the digital identity document and of the e-residence card as well as servicing of the Certificates are continually carried out in accordance with the relevant requirements of the current Policy. Hence, the provisions on the Certificate re-key for validity extension and related provisions thereto, the provisions on Certificates suspension, termination of suspension, revocation and issuance of replacement PIN-codes continue to apply. Certificate re-key to extend the validity of the digital identity document and of the e-residence card is performed under this Policy until the validity of all the relevant documents has been extended. The Certificates are served in accordance with the Certificate Policy until the validity of the last Certificate pair issued under this Policy. Replacement PIN-codes are issued under this Policy until all the remaining envelopes containing PIN-codes have been used up.

	Clause 1.6.1 - Specified CRL definition. Clause 4.7.3 - Added that in case of Certificate re-key for validity extension, identification of the Subscriber SHALL comply with the assurance level high according to eIDAS [2]. Clause 4.9.1 - Specified circumstances for Certificate revocation and added that revoked Certificate shall not be reinstated.
01.11.2018 8.0	Added that Certificate re-key may be done for validity extension of Digi-ID. Therefore, clauses 4.7, 4.7.1, 4.7.2 and 4.7.3 of this CP have been amended accordingly.
01.11.2017 7.0	Due to change of SK's business name from AS Sertifitseerimiskeskus to SK ID Solutions AS, name of the CP has been changed accordingly. Also, former business name has been replaced with the new one in clauses 1.1, 1.2, 1.5.1 and 1.6.2 of this CP. Clause 1.1 - Removed paragraph which stated that the CP a complete redesign of the previous AS Sertifitseerimiskeskus - Certification Practice Statement and ESTEID Card Certification Policy. Clauses 1.1 and 1.3.2 - Lingual corrections. Clause 1.6.2 - Added new acronyms and minor changes. Clauses 4.9.1, 4.9.2, 4.9.3, 4.9.13, 4.9.17, 4.9.18, 4.9.19, 9.15 - Replaced Estonian eIDAS supplement Act with Electronic Identification and Trust Services for Electronic Transactions Act.
01.11.2016 6.0	Redesigned the Certificate Policy in accordance with the IETF RFC 3647 [5] and eIDAS [2].
25.01.2016 5.0	Chapter 1.2 - Changed terminology. Chapter 1.3 - Updated list of Abbreviations. Chapter 1.4 - Changed identification of the Certification Policy. Chapter 1.5.2 - Changed description of Registration Centre. Chapter 1.5.3 - Changed description of PBGB. Chapter 1.5.4 - Changed description of TRÜB. Chapter 1.6 - Changed Contact Details of PBGB. Chapter 2.1.1 - Changed description of SK Obligations. Chapter 2.1.2.1 - Changed description of Obligations of the PBGB Client Service Point. Chapter 2.1.3 - Changed description of Obligations of the PBGB. Chapter 2.1.4 - Changed Obligations of Clients. Chapter 2.5 - Changed description of Audit. Chapter 3.1 - Changed description of Identification of Client. Chapter 4.1 - Changed description of Submission of Applications for Certificates. Chapter 4.2.1 - Changed description of Decision Making. Chapter 4.4 - Changed description of Suspension of Certificates. Chapter 4.5 - Changed description of Termination of Suspension. Chapter 4.6.2 - Changed description of Submission of Application for Revocation. Chapter 6.1.2.1 - Changed description of Creating Client Keys. Chapter 9 - Updated the list of Referred and Related Documents.

	According to changes in certificate renewal and exchange procedure following chapters are also changed: Chapter 2.1.2.2 - Obligations of the SK Client Service Point; Chapter 3.2 - Procedure of Certifying Correspondence of Applicant's Private Key to Public Key. Chapter 4.2.2 - Issuing Certificates. Chapter 4.2.3 - Issuance of the ID card, the RP card and the Digi-ID. Activation of the Certificates. Chapter 4.2.5 - Certificate Renewal and Exchange.
01.12.2014 4.0	Editorial corrections and improvements to document formatting. Adjusted the document content description. Chapter 1.2 - Updated with new terms of E-resident digi-ID, ID-1 format. Chapter 1.6 - Updated contact details of SK and PBGB. Chapter 2.1.2 and 2.1.3 improved obligations of registration centre and PBGB. Chapter 2.4.2 - Updated publication frequency of Certificate Revocation List. Chapter 4.6.1 - Updated authority to revoke certificates. Chapter 6.1.2.1 - Specified creation of client keys. Chapter 6.1.2.3 - Improved rules of activation of client's private key.
01.09.2012 3.3	Added exchange of certificates for ID cards and RP cards that are issued on the year 2011. Chapter 1.2 - Updated terminology. Chapter 2.1.2 - Improved obligations of the registration centre. Chapter 4.2.5 - Amended certificate renewal and exchange.
01.01.2011 3.2	New document added – the residence permit card with the associated actions. Chapter 4.2.1 - Specified submission of Digi-ID certificate applications. Chapter 4.2.3 - Amended certificate activation, certificates are activated immediately, in the presence of the client. Chapter 4.2.5 - Specified certificate updating and permissibility of actions for different documents. Chapter 6.1.2.1 - Specified creation of client keys.
01.10.2010 3.1	Added the requirements applicable to digital personal identification and the 2 OID value assigned to the document.
01.01.2010 2.2	Organisational changes: CMB is now known as PBGB (Police and Border Guard Board) PBGB and SK addresses renewed
28.08.2009 2.1	Combined with the renewed CPS of the SK. Lingual corrections. Updated chapter 1.5.1 - Specified role distribution between different organisations. Updated chapter 4.2.3 - The certificates are being activated within 1 hour subsequent to issuance of the ID card.
19.06.2006 2.0	Updates according to the structure of the new ID card contract.

17.10.2002 1.2	Combined with the CPS of the SK. Amended with topics of certificate renewal and change of the PIN codes of the ID card.
10.11.2001 1.1	First public edition.
Effective from date	10.04.2020

1. Introduction

1.1. Overview

This document, named "SK ID Solutions AS – Certificate Policy for Digi-ID" (hereinafter referred to as CP), defines procedural and operational requirements that SK ID Solutions AS adheres to and requires entities to adhere to when issuing and managing Certificates for the digital identity document as well as for the e-residence cards (hereinafter together referred to as Digi-ID) issued by the Republic of Estonia. These Certificates facilitate electronic signatures and electronic identification of natural persons. The Certificates always come in pairs: each Digi-ID contains one Authentication Certificate and one Qualified Electronic Signature Certificate and their corresponding Private Keys. Each Private Key is protected by separate Activation Data (PIN code) and each Digi-ID has a single Unlock (PUK) code. A single person can have only one valid Digi-ID at any point in time. Digi-ID is physically shaped in ID-1 format, comply to the ISO/IEC 7816 [1] and ID Card documentation [15]. Issuing and managing Certificates for Digi-ID is based on the Regulation (EU) N° 910/2014 [2] which establishes a legal framework for electronic signatures.

This document describes only restrictions to Policy for EU qualified certificate issued to natural persons where the private key and the related certificate reside on a QSCD (QCP-n-qscd) from ETSI EN 319 411-2 [4] and Normalized Certificate Policy requiring a secure cryptographic device (NCP+) from ETSI EN 319 411-1 [3].

The semantics of "no stipulation" in this document is that no additional restrictions are set and relevant provisions from QCP-n-qscd and NCP+ are applied directly.

Issuing and managing Qualified Electronic Signature Certificates for Digi-ID is based on the requirements of the Policy QCP-n-qscd: Certificate Policy for EU qualified Certificates issued to natural persons with Private Key related to the certified Public Key in a QSCD.Issuing and managing Authentication Certificates for Digi-ID is based on the requirements of the Policy NCP+: Normalised Certificate Policy requiring a Secure Cryptographic Device. The Certification Service for Qualified Electronic Signature Certificates for Digi-ID described in this CP SHALL be qualified trust service according to the Trusted List of Estonia. Data structures and communication protocols in use SHALL be described in ID Card documentation [15] where applicable. In case of conflicts, the following documents SHALL be considered in the following order (prevailing ones first):

- QCP-n-qscd
- NCP+
- This CP
- CPS

To preserve IETF RFC 3647 [5] outline this CP is divided into nine parts, section headings that do not apply, are designated as "**Not applicable**". Each top-level chapter includes references to the relevant sections in ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4]. In this CP modal verbs in

capital letters are to be interpreted as described in Clause 3.2 of the ETSI Drafting Rules [6] (Verbal forms for the expression of provisions). Terms and acronyms listed in Clause 1.6 of this CP, are written starting with a capital letter in this CP.

1.2. Document Name and Identification

Refer to Clause 5.3 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4]. This document is named “SK ID Solutions AS – Certificate Policy for Digi-ID". This CP is identified by OID: 1.3.6.1.4.1.10015.1.2. OID is composed according to the contents of the following table.

Parameter	OID reference
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	1.2

Qualified Electronic Signature Certificate for Digi-ID issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-2 [4] clause 5.3 c) for 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)
- This CP.

Authentication Certificates for Digi-ID issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-1 [3] clause 5.3 b) for NCP+: 0.4.0.2042.1.2
- itu-t(0) identified-organization(4) etsi(0)
- other-certificate-policies(2042)
- policy-identifiers(1) ncpplus (2)
- This CP.
-

1.3. PKI Participants

Refer to Clause 5.4 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

1.3.1. Certification Authorities

No stipulation.

1.3.2. Registration Authorities

The RA-s are laid down in Chapter 3 of the IDA [7].
NOTE: The PBGB and Ministry of Foreign Affairs CAN appear in multiple roles throughout the document.
Throughout the rest of this CP a following distinction is made based on the role:

- Both institutions are referred as RA when they are performing technical actions such as face to face
- authentication or delivery of Digi-ID
- They are referred together as PBGB when they are representing Republic of Estonia in the role of Document
- Issuer according to IDA [7], e.g. during initial identification of persons or making decisions about their
- eligibility to apply for Digi-ID

1.3.3. Subscribers

Subscriber is the Subject of the Certificate issued under this CP.
Subscriber can be only a natural person entitled by IDA [7].

1.3.4. Relying Parties

Relying Parties are legal or natural persons who are making decisions based on the Certificate.

1.3.5. Other Participants

Card Manufacturer prepares the cards in the factory and provides technical environment for personalisation in the RA office.
Please note: Card Manufacturer is no longer responsible for preparing the cards and providing technical environment for personalisation as the agreement between Card Manufacturer and PBGB covering production and personalisation of Digi-ID as well as issuance and servicing of the Certificates has terminated.

1.4. Certificate Usage

Refer to Clause 5.5 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

1.4.1. Appropriate Certificate Uses

Subscriber Certificates are intended for the following purposes:
Qualified Electronic Signature Certificate is intended for:

- Creating Qualified Electronic Signatures compliant with eIDAS [2].

Authentication Certificate is intended for:

- Authentication
- Encryption
- Secure e-mail

CA Private Keys SHALL NOT be used to sign other types of Certificates except for the following:

- Subscriber Certificates compliant with QCP-n-qscd or NCP+
- OCSP response verification Certificates
- Internal Certificates for technical needs

1.4.2. Prohibited Certificate Uses

The use of the Subscriber Certificates issued under this CP is prohibited for any of the following purposes:

- Unlawful activity (including cyber attacks and attempt to infringe the Certificate or the Digi-ID)
- Issuance of new Certificates and information regarding Certificate validity
- Enabling other parties to use the Subscriber's Private Key
- Enabling the Certificate issued for electronic signing to be used in an automated way
- Using the Certificate issued for electronic signing for signing documents which can bring about

unwanted consequences (including signing such documents for testing purposes)
The Subscriber Authentication Certificate cannot be used to create Qualified Electronic Signatures compliant with eIDAS [2].

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CP is administered by SK.

SK ID Solutions AS
Registry code 10747013
Pärnu Ave 141, 11314 Tallinn
Tel +372 610 1880
Fax +372 610 1881
Email: info@sk.ee
http://www.sk.ee/en/

1.5.2. Contact Person

Business Development Manager
Email: info@sk.ee

1.5.3. Person Determining CPS Suitability for the Policy

No stipulation.

1.5.4. CP Approval Procedures

Amendments which do not change the meaning of this CP, such as spelling corrections, translation activities
and contact details updates, are documented in the Versions and Changes section of the present document.
In this case the fractional part of the document version number SHALL be enlarged.
In the case of substantial changes, the new CP version SHALL be clearly distinguishable from the previous ones,
and the serial number SHALL be enlarged by one. The amended CP along with the enforcement date, which cannot
be earlier than 30 days after publication, SHALL be published electronically on SK website.
All amendments to this CP SHALL be coordinated with PBGB and Card Manufacturer.

SK performs annual review of this CP to ensure compliance of the present document and Certification service provided under this CP with the applicable requirements.
All amendments SHALL be approved by the business development manager and amended CP SHALL be enforced by the CEO.

1.6. Definitions and Acronyms

1.6.1. Terminology

In this CP the following terms have the following meaning.

Term	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
Card Manufacturer	Prepares the Digi-ID cards in the factory and provides technical environment for personalisation in the RA office.
Certificate	Public key, together with some other information, laid down in the Certificate Profile [8], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of SK structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certificate Revocation List	A list of invalid (revoked, suspended) Certificates. CRL contains suspended and revoked Certificates during their validity period, i.e. until they expire.
Certification Service	Trust service related to Issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates.
Directory Service	Trust service related to publication of Certificate validity information.
Distinguished name	Unique Subject name in the infrastructure of Certificates.
Digi-ID	Digital Identity Document.

Term	Definition
Encrypting	Information treatment method changing the information unreadable for those who do not have necessary skills or rights.
ID-1	Format which defines physical characteristics of identification cards according to standard ISO/IEC 7816 [1].
Integrity	A characteristic of an array: information has not been changed after the array was created.
Object Identifier	An identifier used to uniquely name an object (OID).
Personal Data File	File on Digi-ID that includes the Subscriber's personal data.
PIN code	Activation code for the Authentication Certificate and for the Qualified Electronic Signature Certificate.
Private key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a key pair that may be publicly disclosed by the holder of corresponding Private Key and that is used by Relying Party 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.
PUK code	The unblocking of PIN codes when they have been blocked after number of allowed consecutive incorrect entries.
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 the eIDAS [2] 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.
Qualified Electronic Signature Creation Device	A Secure Signature Creation Device that meets the requirements laid down in eIDAS [2] Regulation.
Relying Party	Entity that relies upon the information contained within a Certificate.
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.

Term	Definition
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.
Subscriber	A natural person to whom Digi-ID Certificates are issued as a public service if he/she has a statutory right.
Subject	In this document, the Subject is the same as the Subscriber.
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 [9] upon receipt the Certificates.

1.6.2. Acronyms

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
eIDAS	Regulation (EU) No 910/2014 [2] 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 [7]
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [3]
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PBGB	Police and Border Guard Board
PKI	Public Key Infrastructure
QSCD	Qualified Electronic Signature Creation Device
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD from ETSI EN 319 411-2 [3]
RA	Registration Authority

Acronym	Definition
SK	SK ID Solutions AS

2. Publication and Repository Responsibilities

Refer to Clause 6.1 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

2.1. Repositories

SK SHALL ensure that its repository is available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0,5% annually.

2.2. Publication of Certification Information

2.2.1. Publication and Notification Policies

This CP, the Certification Practice Statement [16], the Certificate Profile [8], as well as the Terms and Conditions [9] with the enforcement dates, SHALL be published on SK website https://sk.ee/en/repository/ no
less than 30 days prior to taking effect.

2.2.2. Items not Published in the Certification Practice Statement

Information about service levels, fees and technical details laid out in mutual agreements between SK, PBGB and Card Manufacturer MAY be left out of CPS. The CPS MAY not cover internal procedures of the PBGB and Card Manufacturer.

2.3. Time or Frequency of Publication

No stipulation.

2.4. Access Controls on Repositories

No stipulation.

3. Identification and Authentication

Refer to Clause 6.2 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

3.1. Naming

The Distinguished Name of the Certificate SHALL comply with conventions set in the Certificate Profile [8].

3.1.1. Types of Names

No stipulation.

3.1.2. Need for Names to be Meaningful

All the values in the Subscriber information section of a Certificate SHALL be meaningful.

3.1.3. Anonymity or Pseudonymity of Subscribers

Not applicable.

3.1.4. Rules for Interpreting Various Name Forms

Pursuant to IDA [7], international letters SHALL be encoded according to ICAO transcription rules where necessary.
Rules for generating e-mail addresses SHALL be as listed in clause 6.1 of the Certificate Profile [8].

3.1.5. Uniqueness of Names

SK SHALL ensure that Certificates with matching Common Name (CN), SerialNumber and e-mail addresses in
Subject Alternative Name (SAN) fields are not issued to different Subscribers.

3.1.6. Recognition, Authentication, and Role of Trademarks

Not applicable.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Private Keys SHALL be generated on the QSCD during personalisation by the PBGB.

3.2.2. Authentication of Organization Identity

Not applicable.

3.2.3. Authentication of Individual Identity

Authentication is carried out by RA in accordance with Chapter 3 of IDA [7].

3.2.4. Non-Verified Subscriber Information

Non-verified Subscriber information SHALL NOT be allowed in a Certificate.

3.2.5. Validation of Authority

Validation is carried out by RA in accordance with IDA [7].

3.2.6. Criteria for Interoperation

No stipulation

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Subscriber SHALL be identified using the valid Authentication Certificate of Digi-ID that needs to be re-keyed or according to Clause 3.2 of this CP.

3.3.2. Identification and Authentication for Re-Key After Revocation

Refer to Clause 3.2 of this CP.

3.4. Identification and Authentication for Revocation Request

No stipulation.

4. Certificate Life-Cycle Operational Requirements

Refer to Clause 6.3 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

The eligibility for persons to request Digi-ID is defined in IDA [7]. SK SHALL accept CSRs only from the Card Manufacturer.

4.1.2. Enrolment Process and Responsibilities

The responsibilities and process for making decisions about eligibility to apply for a Certificate are laid out in IDA [7]. It is the responsibility of Card Manufacturer to manufacture Digi-ID and initialize the card with correct version of firmware and visual layout. Upon a positive decision PBGB WILL personalise a new Digi-ID, fill out Personal Data File, generate key pairs for Authentication and Qualified Electronic Signature and submit a pair of CSRs to Card Manufacturer. Card Manufacturer forwards the Certificate request to SK. PBGB is responsible for submitting correct identification data (names, personal codes, dates) to the Card Manufacturer. The Card Manufacturer and SK will rely upon the values provided by PBGB. SK is responsible for assigning the correct e-mail address in the eesti.ee domain to the Certificate for Authentication:

- Re-use the previous one if the Subscriber already has an address assigned
- Generate a previously unused address according to clause 6.1 of the Certificate Profile [8] if the Subscriber has a new name
- Generate a previously unused address according to clause 6.1 of the Certificate Profile [8] if the Subscriber has not been previously assigned an address

SK is responsible for keeping track of e-mail address assignments.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The Subscriber's identity WILL be validated by PBGB as described in Chapter 3 of IDA [7].
PBGB WILL send the Certificate requests to SK via the Card Manufacturer.
SK SHALL accept CSRs only from the Card Manufacturer. SK and the Card Manufacturer SHALL rely upon identification data provided by PBGB.

4.2.2. Approval or Rejection of Certificate Applications

CA SHALL refuse to issue a Certificate if the Certificate request does not comply with the technical requirements set in applicable agreements.
If the data contained in a CSR needs to be modified, the corresponding amendment SHALL be coordinated with PBGB.

4.2.3. Time to Process Certificate Applications

In accordance with the applicable laws and agreements.

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

CA SHALL allocate correct and unique e-mail address in the eesti.ee domain to the Subscriber. At this stage, OCSP service SHALL NOT return response "GOOD" and the Certificate SHALL NOT be made available via the Directory Service.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

No stipulation.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2. Publication of the Certificate by the CA

Certificate SHALL be published by the CA using the Directory Service immediately after the Subscriber has accepted it, OCSP SHALL start responding with "GOOD".

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

No stipulation.

4.5.2. Relying Party Public Key and Certificate Usage

No stipulation.

4.6. Certificate Renewal

Not allowed.

4.7. Certificate Re-Key

Certificate re-key SHALL be allowed only upon successful personal identification of the Subscriber via physical identity checks or digital Authentication methods. During Certificate re-key, the Certificates to be replaced SHALL be revoked. Certificate re-key MAY be done only upon initial application in the case of Digi-ID manufacturing errors prior to the acceptance of the Certificates. In this case only the last pair of Certificates SHALL be written to the corresponding Digi-ID media and remain valid. Certificate re-key MAY be done to extend the validity of Digi-ID pursuant to Chapter 9 of IDA [7]. All the erroneous or unusable Certificates SHALL be revoked immediately.

4.7.1. Circumstances for Certificate Re-Key

This CP treats recurring Digi-ID application as initial application for Digi-ID. If the Subscriber applies recurring Digi-ID, this request SHALL be processed as an application for a new Digi-ID, and physical authentication SHALL be done.
Certificate re-key is allowed to:

- Replace an expired or broken Digi-ID
- Fix ASN.1 encoding errors in certificates
- Replace SHA-1 signatures with stronger cryptography
- Fix production errors that are discovered during quality checks
- Extend the validity of Digi-ID pursuant to Chapter 9 of IDA [7]

Additional circumstances for Certificate re-key SHALL be agreed upon with PBGB. CP and CPS SHALL be updated to reflect the changes.

4.7.2. Who May Request Certification of a New Public Key

Only the Subscriber and the Card Manufacturer together CAN initiate the re-key process unless the need to replace the Certificate is discovered during quality checks before the delivery of the Digi-ID to the Subscriber.
SK SHALL NOT accept re-key requests from other parties except for the Card Manufacturer.

4.7.3. Processing Certificate Re-Keying Requests

If the re-keying is to replace an expired or broken Digi-ID or to apply recurring Digi-ID application, the process is similar to initial issuance.

Otherwise the Certificate re-Keying requests SHALL be processed in an automated manner using secure channels for communication. Prior to issuing new Certificates the Subscriber SHALL be Authenticated by using the Private Key corresponding to the valid Authentication Certificate to be replaced. The new Certificates SHALL be written to Digi-ID media.

In case of Certificate re-key for validity extension of Digi-ID, identification of the Subscriber SHALL comply with the assurance level high according to eIDAS [2].

In case of validity extension of Digi-ID, the Card Manufacturer SHALL verify that the data in the Certificates matches the data in the application for the Certificates.

The old Certificates SHALL be revoked immediately. Both Digi-ID Certificates SHALL be replaced simultaneously.

4.7.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Refer to Clause 4.4.1 of this CP.

4.7.6. Publication of the Re-Keyed Certificate by the CA

Refer to Clause 4.4.2 of this CP.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

Refer to Clause 4.4.3 of this CP.

4.8. Certificate Modification

Certificate modification SHALL be allowed only upon successful personal identification of the Subscriber via physical identity checks or digital Authentication methods.

During Certificate modification, the Certificates to be replaced SHALL be revoked. Certificate modification MAY be done only upon initial application in the case of Digi-ID manufacturing errors prior to the acceptance of the Certificates. In this case only the last pair of Certificates SHALL be written to the corresponding Digi-ID media and remain valid. All the erroneous or unusable Certificates SHALL be revoked immediately.

4.8.1. Circumstances for Certificate Modification

Certificate modification is allowed to:

- Change the data that is visually imprinted on the Digi-ID and stored in the Personal Data File
- Change e-mail addresses written to Subject Alternative Name field of the Authentication Certificate
- Fix ASN.1 encoding errors in certificates
- Replace SHA-1 signatures with stronger cryptography
- Fix production errors that are discovered during quality checks

Additional circumstances for Certificate modification SHALL be agreed upon with PBGB. CP and CPS SHALL be updated to reflect the changes.

4.8.2. Who May Request Certificate Modification

Subscriber and the Card Manufacturer together CAN initiate the modification process. In case the need to replace the Certificate is discovered during quality checks before the delivery of the Digi-ID to the Subscriber Certificate Modification MAY be performed by the CA internally or requested by PBGB or Card Manufacturer.

SK SHALL NOT accept modification requests from other parties except for the Card Manufacturer.

4.8.3. Processing Certificate Modification Requests

In case of fixing production errors CA SHALL process Certificate modification requests and is not required to negotiate it with the Subscriber.

In case of changing the data that is visually imprinted on the Digi-ID and stored in the Personal Data File this request SHALL be processed as an application for a new Digi-ID, and physical authentication SHALL be done.

Otherwise the Certificate modification requests SHALL be processed in an automated manner using secure channels for communication. Prior to issuing new Certificates the Subscriber SHALL be authenticated by using the Private Key corresponding to the valid Authentication Certificate to be replaced. The new Certificates SHALL be written to the Digi-ID. The old Certificates SHALL be revoked immediately. Both certificates on the Digi-ID SHALL be replaced simultaneously.

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6. Publication of the Modified Certificate by the CA

Refer to Clause 4.4.2 of this CP.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Refer to Clause 4.4.3 of this CP.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Circumstances for Certificate revocation SHALL be as laid down in IDA [7] and Article 19 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

In addition to the circumstances in the referred laws and more precisely, SK has the right to revoke the Certificate if one or more of the following occurs:

- The Subscriber requests revocation via RA
- SK obtains evidence that the Subscriber has lost control over Private Keys or PIN codes
- SK obtains evidence that the Subscriber's original Certificate request was not authorised and the Subscriber does not retroactively grant authorisation
- 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
- SK obtains evidence that the Certificate was misused
- SK obtains evidence that the used cryptography is no longer ensuring the binding between the Subject and the Public Key
- SK is made aware that the Subscriber has violated one or more of their obligations under the Terms and Conditions [9]
- SK is made aware of a material change in the information contained in the Certificate
- SK is made aware that the Certificate was not issued in accordance with the CP and/or CPS
- SK determines that any of the information appearing in the Certificate is inaccurate or misleading
- SK terminates provisioning of the Certification Service or SK is dissolved
- SK is made aware of a possible compromise of the Private Key of the SK CA used for issuing the Certificate
- Revocation is required by the CP
- The technical content or format of the Certificate presents an unacceptable risk to Relying Parties
- If such an obligation is foreseen by the law or any legislation established on the basis thereof

Revoked Certificate SHALL NOT be reinstated.

4.9.2. Who Can Request Revocation

Entities eligible to request Certificate revocation SHALL be as laid down in IDA [7] and Article 19 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

4.9.3. Procedure for Revocation Request

The procedure for revocation request SHALL be as laid down in IDA [7] and Article 20 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

4.9.4. Revocation Request Grace Period

No stipulation.

4.9.5. Time Within Which CA Must Process the Revocation Request

No stipulation.

4.9.6. Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7. CRL Issuance Frequency

No stipulation.

4.9.8. Maximum Latency for CRLs

No stipulation.

4.9.9. On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10. On-Line Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

No stipulation.

4.9.13. Circumstances for Suspension

Circumstances for Certificate suspension SHALL be as laid down in Article 17 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

4.9.14. Who Can Request Suspension

Anyone can request Certificate suspension.

4.9.15. Procedure for Suspension Request

It SHALL be possible to request Certificate suspension via phone 24 hours a day, 7 days a week. Certificate suspension SHALL leave a uniquely identifiable trace.

4.9.16. Limits on Suspension Period

No limits.

4.9.17. Circumstances for Termination of Suspension

Circumstances for termination of Certificate suspension SHALL be as laid down in Article 18 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

4.9.18. Who Can Request Termination of Suspension

Entities who can request termination of Certificate suspension SHALL be as laid down in Article 18 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

4.9.19. Procedure for Termination of Suspension

The procedure for termination of Certificate suspension SHALL be as laid down in Article 18 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

4.10. Certificate Status Services

4.10.1. Operational Characteristics

No stipulation.

4.10.2. Service Availability

SK SHALL ensure that its Certificate Status Services are available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0,5% annually.

4.10.3. Operational Features

No stipulation.

4.11. End of Subscription

No stipulation.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

Not allowed.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

Refer to Clause 6.4 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

6. Technical Security Controls

Refer to Clause 6.5 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The Subscriber Certificate keys SHALL be generated using the QSCD by one of the following roles:

- Subscriber
- PBGB

6.1.2. Private Key Delivery to Subscriber

Certificate keys SHALL be delivered on a QSCD that SHALL be handed over to the Subscriber by the PBGB.

6.1.3. Public Key Delivery to Certificate Issuer

PBGB SHALL deliver the Public Key to the Card Manufacturer using a secure communication channel.
The Card Manufacturer SHALL deliver the Public Key to the CA using a secure communication channel.

6.1.4. CA Public Key Delivery to Relying Parties

No stipulation.

6.1.5. Key Sizes

Allowed key sizes SHALL be as described in the Certificate Profile [8].

6.1.6. Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

Allowed key usage flags SHALL be set as described in the Certificate Profile [8].

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Private Key SHALL be generated on a QSCD.

6.2.2. Private Key (n out of m) Multi-Person Control

No stipulation.

6.2.3. Private Key Escrow

No stipulation.

6.2.4. Private Key Backup

No stipulation.

6.2.5. Private Key Archival

No stipulation.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

No stipulation.

6.2.7. Private Key Storage on Cryptographic Module

No stipulation.

6.2.8. Method of Activating Private Key

The Subscriber SHALL be prompted to enter the PIN code of the Authentication Certificate at least once after the Digi-ID has been inserted into the card reader device.

The Subscriber SHALL be prompted to enter the PIN code of the Qualified Electronic Signature Certificate before every single operation done with the corresponding Private Key.

It SHALL be possible to create different PIN codes for different keys of the Subscriber.

The length of the PIN codes SHALL be at least:

- For the Authentication Key 4 numbers
- For the signature Key 5 numbers

The PUK code SHALL be at least 8 numbers.

6.2.9. Method of Deactivating Private Key

No stipulation.

6.2.10. Method of Destroying Private Key

No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

No stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Validity period of the Subscriber Certificate SHALL NOT exceed the validity period of the corresponding Digi-ID for which it was issued.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The initial activation data SHALL be generated by the Card Manufacturer and SHALL be included in a separate sealed envelope for delivery to the Subscriber. Copies of the PIN codes SHALL NOT be stored by the Card Manufacturer.

The Card Manufacturer SHALL produce replacement PIN codes and SHALL hand them over to RA in sealed envelopes. The mechanism for replacing the activation data SHALL ensure by technical means the impossibility to view or store the replacement activation data by the RA employee during the whole process.

RA SHALL issue replacement PIN codes to the Subscriber when the PIN codes need to be replaced or updated.

All PIN codes of a single Digi-ID are replaced at once.

Prior to issuing replacement PIN codes the RA SHALL Authenticate the Subscriber.

6.4.2. Activation Data Protection

PIN codes SHALL be handed over personally to the Subscriber by the RA.
Copies of the PIN codes SHALL NOT be stored by the RA.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

No stipulation.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

No stipulation.

6.6.2. Security Management Controls

No stipulation.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

No stipulation.

6.8. Time-Stamping

No stipulation.

7. Certificate, CRL, and OCSP Profiles

Refer to Clause 6.6 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

7.1. Certificate Profile

The Certificate SHALL comply with the profile described in the Certificate Profile [8].

7.2. CRL Profile

The CRL SHALL comply with the profile described in the Certificate Profile [8].

7.3. OCSP Profile

The OCSP responses SHALL comply with the profile described in the Certificate Profile [8].

8. Compliance Audit and Other Assessments

Refer to Clause 6.7 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

No stipulation.

9.1.2. Certificate Access Fees

No stipulation.

9.1.3. Revocation or Status Information Access Fees

No stipulation.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

No stipulation.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. Confidentiality of Business Information

No stipulation.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

No stipulation.

9.4.2. Information Treated as Private

No stipulation.

9.4.3. Information Not Deemed Private

No stipulation.

9.4.4. Responsibility to Protect Private Information

No stipulation.

9.4.5. Notice and Consent to Use Private Information

No stipulation.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property rights

SK obtains intellectual property rights to this CP.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

An employee of CA SHALL NOT be punished for an intentional crime.

9.6.2. RA Representations and Warranties

An employee of RA SHALL NOT be punished for an intentional crime.

9.6.3. Subscriber Representations and Warranties

No stipulation.

9.6.4. Relying Party Representations and Warranties

Relying Party SHALL verify the validity of the Certificate using validation services offered by SK prior to using the Certificate.

Relying Party SHALL consider the limitations stated in the Certificate and SHALL ensure that the transaction to be accepted corresponds to this CP.

9.6.5. Representations and Warranties of Other Participants

An employee of the Card Manufacturer SHALL NOT be punished for an intentional crime.

9.7. Disclaimers of Warranties

No stipulation.

9.8. Limitations of Liability

No stipulation.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

Refer to Clause 2.2.1 Publication and Notification Policies of this CP.

9.10.2. Termination

This CP SHALL remain in force until it is replaced by the new version or when it is terminated due to the CA termination or when the service is terminated and all the Certificates therefore become invalid.

9.10.3. Effect of Termination and Survival

SK SHALL communicate the conditions and effect of termination of this CP.

9.11. Individual Notices and Communications with Participants

No stipulation.

9.12. Amendments

9.12.1. Procedure for Amendment

Refer to Clause 1.5.4 of this CP.

9.12.2. Notification Mechanism and Period

Refer to Clause 1.5.4 of this CP.

9.12.3. Circumstances Under Which OID Must be Changed

OID SHALL change when the scope of this CP changes or when the new type of the Certificate occurs.

9.13. Dispute Resolution Provisions

No stipulation.

9.14. Governing Law

This CP is governed by the jurisdictions of the European Union and Estonia.

9.15. Compliance with Applicable Law

SK SHALL ensure compliance with the following requirements:

- eIDAS [2] - 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
- Electronic Identification and Trust Services for Electronic Transactions Act [10]

- Identity Documents Act [7]
- State Fees Act [11]
- Personal Data Protection Act [12]

related European Standards:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [13]
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [3]
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates [4]
- EN 419 211 Protection profiles for secure signature creation device [14]

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

No stipulation.

9.16.4. Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5. Force Majeure

No stipulation.

9.17. Other Provisions

Not allowed.

10. References

1. ISO/IEC 7816, Parts 1-4, published: http://iso.org/;
2. 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;
3. ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
4. ETSI EN 319 411-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates;

5. RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, published: https://www.ietf.org/rfc/rfc3647.txt;
6. ETSI Drafting Rules (Verbal forms for the expression of provisions);
7. Identity Documents Act, RT I 1999, 25, 365, published: https://www.riigiteataja.ee/en/eli/511042016001/consolide/current;
8. Certificate, CRL and OCSP Profile for personal identification documents of the Republic of Estonia, published: https://sk.ee/en/repository/profiles/;
9. Terms and Conditions for Use of Certificates of Personal Identification Documents of the Republic of Estonia, published: https://sk.ee/en/repository/conditions-for-use-of-certificates/;
10. Electronic Identification and Trust Services for Electronic Transactions Act, 26.10.2016, published:https://www.riigiteataja.ee/en/eli/527102016001/consolide/current;
11. State Fees Act, published: https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current;
12. Personal Data Protection Act, 06.01.2016, published: https://www.riigiteataja.ee/en/eli/507032016001/consolide/current;
13. ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
14. ETSI EN 419 211 Protection profiles for secure signature creation device;
15. ID card documentation webpage: http://www.id.ee/index.php?id=35772;
16. SK ID Solutions AS - ESTEID-SK Certification Practice Statement, published: https://www.sk.ee/repositoorium/CPS/.