ESTEID Certification Policy

Version 2.2
OID: 1.3.6.1.4.1.10015.1.1.2.2
Valid from 01.01.2010

Requirements on the national ID-card of the Republic of Estonia with the purpose of issuing and service certificates which facilitate digital signature and identification of persons.

Version information		
Date	**Version**	**Changes/Updates/Amendments**
01.01.2010	2.2	Organizational 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 organizations. 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.

Table of Contents

1. Introduction

1.1. Overview

This document (hereinafter Certificate Policy, CP) is a set of rules which specifies the fundamental operating principles and concepts of the certification service provision essential for digital signature and person identification certificates' issuance for the EstEID card (hereinafter the ID-card).

This CP is based on the document titled "AS Sertifitseerimiskeskus – Certification Practice Statement" [1] which is registered in Registry of Certification Services (RCS). This Certification Practice Statement (hereinafter the CPS) shall serve as a basis for supply of certification service. This CP supplements the principles set out in the CPS for ID-card certification services.

In the case of conflict between the CP and the CPS the provisions of this CP shall prevail. In case of conflict between the Estonian original document and the English translation the Estonian original shall prevail.

This CP extends only to the digital certificates issued by AS Sertifitseerimiskeskus.

IETF (Internet Engineering Task Force) recommended document RFC 2527 [4] has been used in drafting this CP.

1.2. Terminology

Term	Definition
Client Service Point	Client Service Point of SK and/or PBGB action under this CP providing services described in this CP, refer to chapter 1.5.2.1.
Terms of use of the certificates of ID-card.	Document that describes the obligations and responsibilities for the Client while using ID-card and its digital certificates. Client has to be familiar with its contents and accept the terms and conditions described within.

1.3. Abbreviations

Abbreviation	Definition
PBGB	Police and Border Guard Board
IM	Estonian Ministry of the Interior
TRÜB	TRÜB AG, ID-card producer and personalizer

SK	AS Sertifitseerimiskeskus, certification authority
CA	Certification authority registered in RCS

1.4. Identifying the Certification Policy

This CP is identified by **OID: 1.3.6.1.4.1.10015.1.1.2.2**

The OID code of this CP is added to certificates issued under this CP.

The OID is composed as described in Table 1.

Parameter	**OID section**
Internet attribute	1.3.6.1
Private business attribute	4
Registered business attribute given by private business manager IANA	1
SK attribute in IANA register	10015
Certification service attribute	1.1
CP version attribute	2.2

Table 1. Composition of the CP identification code

1.5. Organization and Area of Application

1.5.1. Sertifitseerimiskeskus (SK)

Refer to CPS p.1.2.1.

The certificates are issued to the ID-card. The issuance of ID-card is a responsibility of PBGB. There is a contract signed between TRÜB and PBGB covering production, personalization of ID-cards as well as issuance and servicing of the certificates. The contract signed between SK and TRÜB states that SK will act as a CA. According to the contract signed between TRÜB and PBGB, the obligations described in chapters 1.5.2 and 1.5.3 are delegated to PBGB.

1.5.2. SK Registration Centre

1.5.2.1. Client Service Point

Refer to CPS p.1.2.2.1.

Accepting applications and issuance of the ID-cards is carried out in PBGB regional offices, bureaus and embassies of the Republic of Estonia (hereafter PBGB client service point). The list and operating hours of client service points is published on the websites of SK and PBGB.

Servicing certificates of ID-cards (renewals, suspensions, terminations of suspension, revocations and designations of the replacement PIN envelopes) is carried out in client service points referred with operation hours on the websites of PBGB and SK.

1.5.2.2. Help Line

Refer to CPS p.1.2.2.2.

For identification checks Help Line uses internally documented procedures. Help Line also provides user support for solving problems related to ID-card usage.

1.5.3. PBGB

PBGB:

- Forwards the ID-card production orders to TRÜB;
- Forwards the personalized ID-cards to the client service points.

PBGB will follow the time limits described in contract.
While providing the service, PBGB will ensure the security with its internal security procedures.

1.5.4. Card Personalizer – TRÜB

TRÜB:

- Accepts ID-card orders;
- Personalizes the ID-card;
- Generates the keys for ID-card and requests the corresponding certificates;
- Loads the certificates to the ID-card;
- Delivers the personalized ID-cards to the PBGB.

TRÜB will follow the time limits described in contract.
While providing the service, TRÜB will ensure the security with its internal security procedures.

1.5.5. User

1.5.5.1. Client

Refer to CPS p.1.2.3.1.

Client is a physical person the ID-card certificates are issued to as a public service if he/she has a statutory right.

Client is the holder of the certificate issued under this CP.

Client’s distinguished name is compiled according to the certificate profile described in document “Certificates on the National ID-card of the Republic of Estonia”.

The Client has to have an opportunity to get acquainted with the terms and conditions of usage of ID-card certificates [5].

1.5.5.2. Relying Party

Refer to CPS p.1.2.3.2.

1.5.6. Area of Application of Certificates

Refer to CPS p.1.2.4.

There are two types of certificates issued under this CP:

a) Certificates for digital signature.
b) Certificates for digital identification of persons.

Certificates for digital signature can be used for digital signature as defined in the Digital Signatures Act [3].

This CP does not limit the use of the certificates issued in different software applications or fields of application.

1.6. Contact Details

Refer to CPS p.1.3.

SK

AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu mnt 141, 11314 Tallinn
Phone +372 610 1880
Fax +372 610 1881
E-mail: pki@sk.ee
http://www.sk.ee

Help Line

Phone 1777, +372 677 377

Client Service Points

Client service points are cited on the websites http://www.sk.ee and http://www.politsei.ee

PBGB

Pärnu mnt 139
15060 Tallinn
Customer Help Line: 612 3000
Phone: 612 3300
Fax: 612 3009
E-mail: ppa@politsei.ee

The change of contact details is immediately announced on the website of the SK http://www.sk.ee and on PBGB website http://www.politsei.ee

TRÜB

Trüb Baltic AS
Liivalaia 8
10118 Tallinn
Phone +372 613 29 11
Fax +372 613 29 20
E-mail info@trueb.ee

2. General Terms

2.1. Obligations

2.1.1. Obligations of SK

Refer to CPS p.2.1.1.

SK shall warrant in addition that:

- The certification service is provided in accordance with the Certification Practice Statement of AS Sertifitseerimiskeskus;
- The certification service is provided in accordance with this CP.

SK hereby additionally undertakes to:

- Accept certificate requests from TRÜB and issue the respective certificates;
- Supply the directory service 24 hours a day;
- Ensure that the certification keys used are protected by hardware security modules and under sole control of SK;
- Suspending all the certificates issued in case of compromise of the certification keys;
- Ensure that all activated certification keys are located within the borders of the Republic of Estonia;
- Ensure that the signing keys used in the supply of certification service are activated on the basis of shared control;
- Adhere to the time limits established by the contract.

2.1.2. Obligations of the Registration Centre

2.1.2.1. Obligations of the PBGB Client Service Point

Refer to CPS p.2.1.2.1.

PBGB Client Service Point additionally undertakes to:

- Issue ID-card to the Client by first activating the certificates loaded thereon;
- Ensure initial advice and assistance in handling the ID-cards.

2.1.2.2. Obligations of the SK Client Service Point

The SK Client Service Point shall accept the applications for renewals, suspensions, terminations of suspension and revocations of the certificates while validating these applications for the correctness and integrity. The Client Service Point obligates to check the applicant's identity as well as the powers to carry out the operations.

The SK Client Service Point shall warrant the required training for its employees for providing the quality service.

The employee of the SK Client Service point may not have been punished for an intentional crime.

2.1.2.3. Obligations of the Help Line

Refer to CPS p.2.1.2.2.

2.1.3. Obligations of the PBGB

PBGB obligates to:

- Within the limits of the information system that is related to the certification system follow the availability and the security requirements which must comply at least with the requirements described in this CP;
- Guarantee that the employees, accepting the ID-card applications and/or are engaged in the information system of the certification service, have not been punished for an intentional crime;
- Send out the ID-cards to be issued in the Embassies of the Republic of Estonia;
- Ensure the availability of the information on the ID-cards in a public data communications network on the website http://www.politsei.ee

2.1.4. Obligations of Clients

Refer to CPS p.2.1.3.

Upon application for an ID-card a Client shall submit to the PBGB true and correct information and in the case of a change in his or her personal details immediately notify the PBGB of the correct details in accordance with the established legislation.

2.1.5. Obligations of Relying Party

Refer to CPS p.2.1.4.

2.1.6. Obligations of Directory Service

Refer to CPS p.2.1.5.

There are no additional obligations specified for providing the service of the Public Directory.

2.2. Liability

2.2.1. Liability of the SK

Refer to CPS p.2.2.1.

SK is liable for all obligations described in chapters 2.1.1 and 2.1.2 of this CP within the limits of legislation of the Republic of Estonia.

2.2.2. Liability of the Registration Centre

2.2.2.1. Liability of the PBGB Client Service Point

Refer to CPS p.2.2.2.1.

PBGB Client Service Point is liable for all obligations described in chapter 2.1.2.1 of this CP.

2.2.2.2. Liability of the SK Client Service Point

Refer to CPS p.2.2.2.1.

SK is liable for all obligations described in chapter 2.1.2.2 of this CP.

2.2.2.3. Liability of the Help Line

Refer to CPS p.2.2.2.2.

SK and PBGB are liable for all obligations described in chapter 2.1.2.3 of this CP.

2.2.3. Liability of the PBGB

PBGB is liable for all obligations described in chapter 2.1.3 of this CP.

2.2.4. Limits of Liability

Refer to CPS p.2.2.3.

2.3. Settling Disputes

Refer to CPS p.2.3.

2.4. Publication of Information and Directory Service

2.4.1. Publication of information by SK

Refer to CPS p.2.4.1.

The valid Certificate Revocation List is accessible on website http://www.sk.ee/crls/esteid/

2.4.2. Publication Frequency

Refer to CPS p.2.4.2.

The Certificate Revocation Lists are published after each 12 hours.

2.4.3. Access Rules

Refer to CPS p.2.4.3.

2.4.4. Directory Service

Refer to CPS p.2.4.4.

The certificates issued under this CP shall be published in public directory at ldap://ldap.sk.ee subsequent to the activation of the certificates.

Suspended and revoked certificates are deleted from the public directory. In case of termination of suspension of a certificate, the certificate shall be re-published in the public directory.

Expired certificates shall be deleted from the public directory on the date subsequent to the date of certificate expiry.

2.5. Audit

Refer to CPS p.2.5.

All the contacts described in chapter 1.5 shall be informed of the results of external audit. The audit results shall also be published on the website of the SK.

2.6. Confidentiality

Refer to CPS p.2.6.

3. Client Identification

3.1. Identification of Client

The identification of the Client is checked in accordance with the legislation.

3.2. Procedure of Certifying Correspondence of Applicant's Private Key to Public Key

The certificates are issued corresponding to the public keys generated during personalization of ID-card by TRÜB based on this CP. During the renewal the certificates are issued corresponding to the public keys generated by Client also based on this CP.

3.3. Distinguished Name

Refer to CPS p.3.3.

The distinguished name of the Client is composed according to the description in document "Certificates on the National ID-card of Republic of Estonia" [2].

4. Provision of Certification Service. Procedure and Terms of Certification Process

4.1. Submission of Applications for Certificates

Refer to CPS p.4.1.

The client fills and signs the ID-card application form. A signed application for an ID-card serves as a basis for the preparation of an application for the certificate.

Additional information is available on these websites: http://www.pass.ee, http://www.mig.ee and http://www.sk.ee.

4.2. Processing of Applications for Certificates

The exact procedure and terms for processing the ID-card applications have been determined by the relevant legislation. Upon processing the applications for the certificate the correctness and completeness of the information supplied by the Client is checked.

4.2.1. Decision Making

Refer to CPS p.4.2.1.

The acceptance or rejection of an application for an ID-card shall be decided by the PBGB. The decision for ID-card with valid certificates is based on the Client's right to have one according to the legislation of the Republic of Estonia.

In case of positive decision, TRÜB shall generate keys for the Client and composes the corresponding certificate requests for issuing one certificate for digital signing and one for digital authentication and forwards the requests to SK for certificate issuance.

SK decides the acceptance or rejection of an application for new pair of certificates for ID-card.

4.2.2. Certificate Issuance

After checking the authenticity and integrity of the certificate request and SK automatically issues the certificates which will be loaded to ID-card in TRÜB.

All issued certificates are in inactive state as they are not available via public directory as described in chapter 2.1.6, but are located in the certificate database in a closed section of SK's information system.

For the ID-card that has valid certificates, the new certificates shall be issued in PBGB or SK Client Service Point or in an application locate on SK's website if an application is filed and accepted.

4.2.3. Issuance of the ID-card, Activation of the Certificates

The ID-card is issued to the Client in the PBGB Client Service Point.

Along with the ID-card issuance, the employee of the PBGB Client Service Point forwards the certificates on this ID-card to the certificate activation queue. The certificates on the ID-card shall be activated within 1 hour since the issuance of the ID-card.

The secure PIN code envelope containing the certificate activation codes will be handed over to the Client by an employee of the PBGB Client Service Point or by an employee of the Embassy of the Republic of Estonia.

The Client (or his/her legal representative) signs the file of ID-card issuance which also confirms the Client's familiarization with the the terms and conditions of usage of ID-card certificates [5].

During the renewal of the certificates, the certificates shall be activated immediately after the certificates are loaded onto the ID-card chip.

4.2.4. Certificate Check-up and Verification

Refer to CPS p.4.2.4.

4.2.5. Certificate Renewal

The certificates that are expired or revoked can be replaced with certificates issued on basis of newly generated key pair.

4.3. Applications for Suspension and Revocation of Certificates

Refer to CPS p.4.3.

4.4. Suspension of Certificates

Refer to CPS p.4.4.

Suspension of certificates is possible also in the Client Service Points of the PBGB.

The identity of the applicant is checked in accordance with the relevant legislation.

The documents data of the applicant used during identity check will be documented while registering an application.

4.5. Termination of Suspension

Refer to CPS p.4.5.

The suspension of certificates can be also terminated in the Client Service Points of PBGB.

The identity of the applicant is checked in accordance with the relevant legislation.

The application for termination of suspension of certificates must include:

- Holder's and applicant's (if the applicant differs from holder) forename and surname;
- The personal id-code of the holder and the applicant (if the applicant differs from holder);
- The basis for terminating of suspension of certificates.

The documents data of the applicant used during identity check will be documented while registering an application in the Client Service Point of PBGB.

4.6. The Certificate Revocation

4.6.1. The Powers of Revoking a Certificate

Refer to CPS p.4.6.1.

PBGB can present an application to revoke a certificate subsequent to revocation of the ID-card.

4.6.2. Submission of Application for Revocation

Refer to CPS p.4.6.2.

Revocation of certificates is also possible in the Client Service Point of the PBGB. The applicant’s identity is checked according to the relevant legislation.

The application for revoking the certificates must contain:

- Holder’s and applicant’s (if the applicant differs from holder) forename and surname;
- The personal id-code of the holder and the applicant (if the applicant differs from holder);
- The basis for terminating of revocation of certificates.

The documents data of the applicant used during identity check will be documented while registering an application in the Client Service Point of PBGB.

4.6.3. Procedure of Revocation

Refer to CPS p.4.6.3.

Revocation of certificates is also possible in the Client Service Point of the PBGB.

4.6.4. Effect of Revocation

Refer to CPS p.4.6.4.

4.7. Procedures Ensuring Tracking

Refer to CPS p,4.7.

4.8. Action in an Emergency

Refer to CPS p.4.8.

4.9. Termination of Certification Service Provider Operations

Refer to CPS p.4.9.

5. Physical and Organizational Security Measures

5.1. Security Management

Refer to CPS p.5.1.

5.2. Physical Security Measures

5.2.1. SK Physical Entrance Control

Refer to CPS p.5.2.1.

5.2.2. Other Requirements. Storage of ID-cards

ID-cards shall be stored in the Client Service Points of PBGB according to the enforced internal security regulations.

Replacement PIN-envelopes shall be stored in the Client Service Points of PBGB and SK according to the enforced internal security regulations.

5.3. Requirements for Work Procedures

Refer to CPS p.5.3.

5.4. Personnel Security Measures

Refer to CPS p.5.4.

6. Technical Security Measures

6.1. Key Management

6.1.1. Certification Keys of SK

Refer to CPS p.6.1.1.

6.1.2. Client Keys

6.1.2.1. Creating the Client Keys

The algorithms, key lengths and other parameters are described in document “Certificates on the National ID-card of Republic of Estonia” [2].

The keys shall be generated during personalization of ID-card and during certificate renewal in the Client Service Points of PBGB and SK. The keys shall be loaded to the security area of the smartcard chip. The generated keys can not be extracted nor restored from the smartcard.

The keys of the Client are protected by the activation PIN codes known only to the Client.

6.1.2.2. Protection of Client's Private Key and Activation Codes during Personalization Period

The confidentiality and non-usage of the generated private keys and activation codes until issuance of ID-card used for storing private keys and activation codes to the Client is warranted by PBGB, SK and TRÜB.

Activation codes shall be printed in one copy straight to the security envelope which is handed over to the Client unopened.

6.1.2.3. Activation of Client's Private Key

Refer to CPS p.6.1.2.3.

Subsequent to insertion of three false activation codes (PIN-codes) the smart card shall be blocked. The PUK-code handed over to the Client can be used for unblocking the smart card.

Subsequent to insertion of three false PUK-codes, the smart card shall be blocked permanently.

If the PUK-codes are lost or the smart card is permanently blocked, the Client has to refer to the Client Service Points of PBGB or SK for a replacement PIN-envelope.

6.1.2.4. Backup and Deposition of Client's Keys

There shall be neither backup nor depositions of the private keys of the Client under any circumstance.

6.2. Logical Security

Refer to CPS p.6.2.

6.3. Description of Technical Means Used for Certification

Refer to CPS p.6.3.

6.4. Storage and Protection of Information Created in Course of Certification

Refer to CPS p.6.4.

7. Technical Profiles of Certificates and Revocation Lists

The technical profiles of certificates and certificate revocation lists (CRL) are described in document “Certificates on the National ID-card of the Republic of Estonia” [2].

8. Management of Certification Policy

Refer to CPS p.8.

This CP and referred documents – the "Certification Practice Statement of AS Sertifitseerimiskeskus" (CPS) [1] and "Certificates on the National ID-card of the Republic of Estonia" [2] shall be published on the website of SK.

The terms and conditions of usage of ID-card certificates [5] shall be published on the websites of SK and PBGB.

All changes are coordinated with PBGB and TRÜB.

9. Referred and Related Documents

Referred documents:

[1] The Certification Practice Statement of AS Sertifitseerimiskeskus (CPS)
[2] EVS 828:2009 „ Certificates on the National ID-card of the Republic of Estonia "
[3] Digital Signatures Act of the Republic of Estonia, RT I 2000, 26, 150
[4] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
[5] The terms and conditions of usage of ID-card certificates.

Related legislation:

- Identity Documents Act, RT I 1999, 25, 365
- Personal Data Protection Act, RT I 2007, 24, 127