BANKA SLOVENIJE
EVROSISTEM

CERTIFICATION PRACTICES STATEMENT OF THE CERTIFICATION AUTHORITY AT THE BANK OF SLOVENIA

Type	GUIDANCE (NAV)
Document ID	2.01.0.1-2/2021-69
Version	3
Custodian	Information technology

»This document contains an unofficial and courtesy English translation of [PKI-Splošni postopki overitelja digitalnih potrdil na Banki Slovenije]. In the event of any ambiguity about the meaning of certain translated terms or of any discrepancy between the Slovenian version of the act and the translation, the Slovenian version shall apply.«

Recipients: This document is labelled a "public document" under the Bank of Slovenia confidentiality classification scheme, and is made publicly available on the Bank of Slovenia website.

References:

- IETF RFC 5280 – "*Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List Profile*"
- PKCS #1 – "*RSA Cryptography Standard*"
- PKCS #10 – "Certification Request Syntax Standard"
- IETF RFC 3647 – "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*"
- ESCB CAF – "*ESCB Certificate Acceptance Framework*"

TABLE OF CONTENTS

1 INTRODUCTION 8

1.1 INFRASTRUCTURE OF THE CA AT THE BS 8
1.2 DOCUMENT NAME AND IDENTIFICATION 9
1.3 PKI PARTICIPANTS 9
1.3.1 Certification Authority at the BS 10
1.3.2 The Policy Approval Authority 10
1.3.3 Certification Authority servers 10
1.3.4 Registration Authority 10
1.3.5 Key Archive 11
1.3.6 Digital certificate users 11
1.4 CERTIFICATE USAGE 11
1.4.1 Appropriate certificate use 11
1.4.2 Prohibited use of certificates 11
1.5 POLICY ADMINISTRATION 12
1.5.1 Contact information 12
1.5.2 Procedures to change the CP and the CPS 12
1.5.3 Person responsible for determining CPS compliance with the CP 13
Defined in the CP under which the digital certificates were issued. 13
1.5.4 Publishing the policy 13
1.6 DEFINITIONS AND ACRONYMS 13

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 13

2.1.1 Frequency of publication 13
2.1.2 Access control on published information 13

3 IDENTIFICATION AND AUTHENTICATION 14

3.1 NAMING 14
3.1.1 Name types 14
3.1.2 The need for names to be meaningful 14
3.1.3 Use of anonymous names and pseudonyms 14
3.1.4 Rules for interpreting various name forms 14
3.1.5 Uniqueness of names 14
3.1.6 Name dispute resolution procedures 15
3.1.7 Recognition, authentication and the role of trademarks 15
3.2 REFER TO THE CORRESPONDING CP FOR THE CERTIFICATE ISSUED.INITIAL IDENTITY VALIDATION 15
3.2.1 Method to prove possession of a private key 15
3.2.2 Validation of the organization's identity 15
3.2.3 Validation of an individual identity 15
3.2.4 Non-verified applicant information 16
3.2.5 Validation of authority 16
3.2.6 External CA interoperation 16
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 16
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS 16

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 17

4.1 CERTIFICATE APPLICATION 17
4.1.1 Who can submit a certificate application 17
4.1.2 Preparing applications and applicant's responsibilities 17
4.2 CERTIFICATE APPLICATION PROCESSING 17
4.2.1 Performing the identification and authentication procedure 17
4.2.2 Approval or rejection of digital certificate applications 18

4.2.3Processing time ... 18
4.3 CERTIFICATE ISSUANCE ... 18
4.3.1Actions performed by the CA during the issuance ... 18
4.3.2Notification mechanisms used by the CA to notify the holder ... 18
4.4 CERTIFICATE ACCEPTANCE ... 19
4.4.1Procedure for accepting the certificate ... 19
4.4.2Publication of the certificate ... 19
4.4.3Notification of certificate issuance by the CA to other entities ... 19
4.5 KEY PAIR AND CERTIFICATE USAGE ... 19
4.5.1Holder's use of the private key and the digital certificate ... 19
4.5.2Relying party use of the public key and the digital certificate ... 19
4.6 CERTIFICATE RENEWAL ... 19
4.7 CERTIFICATE RE-KEY ... 19
4.7.1Circumstances for certificate re-key ... 19
4.7.2Who may request certificate re-key? ... 19
4.7.3Procedure for processing certificate re-key ... 20
4.7.4Notification of re-key to the certificate holder ... 20
4.7.5Acceptance of the certificate ... 20
4.7.6Publication of issued certificate after certificate re-key ... 20
4.7.7Notification of certificate issuance by the CA to relying parties ... 20
4.8 CERTIFICATE MODIFICATION ... 20
4.9 REVOCATION AND SUSPENSION OF DIGITAL CERTIFICATE ... 20
4.9.1Grounds for revocation ... 20
4.9.2Who can request certificate revocation ... 20
4.9.3Procedure used for certificate revocation request ... 20
4.9.4Grace period available to holder to prepare the revocation request ... 21
4.9.5The time within which the CA should process revocation requests ... 21
4.9.6Revocation checking requirements for relying parties ... 21
4.9.7The CRL issuance frequency ... 21
4.9.8Maximum latency between the generation of CRLs and their publication ... 21
4.9.9Online certificate revocation status checking ... 22
4.9.10 Online revocation checking requirements ... 22
4.9.11 Other forms of revocation alerts available ... 22
4.9.12 Special requirements for the revocation of compromised keys ... 22
4.9.13 Grounds for suspension of a digital certificate ... 22
4.9.14 Who can request or cancel the suspension of a digital certificate ... 22
4.9.15 Procedure for suspension of a digital certificate ... 22
4.9.16 Duration of suspension of a digital certificate ... 22
4.10 CERTIFICATE STATUS SERVICES ... 22
4.10.1 Operational characteristics ... 22
4.10.2 Service availability ... 22
4.10.3 Additional features ... 23
4.11 TERMINATION OF THE RELATIONSHIP BETWEEN THE HOLDER AND THE CA ... 23
4.12 KEY ESCROW AND RECOVERY ... 23
4.12.1 Key archive and recovery policies ... 23
4.12.2 Session key protection ... 24

5 MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS ... 24

5.1 PHYSICAL SECURITY CONTROLS ... 24
5.1.1Site location and construction ... 24
5.1.2Physical access ... 25
5.1.3Power and air conditioning ... 25
5.1.4Water exposures ... 25
5.1.5Fire prevention and protection ... 25
5.1.6Media storage ... 26
5.1.7Waste disposal ... 26
5.1.8Off-site backup ... 26
5.2 PROCEDURAL SECURITY CONTROLS ... 26
5.2.1The CA organizational structure and distribution of roles ... 26
5.2.2Number of individuals required per task ... 28

5.2.3Identification and authentication requirements for each role ... 29
5.2.4Roles requiring separation of duties ... 29
5.3 PERSONNEL SECURITY CONTROLS ... 30
5.3.1Qualifications, experience and authorization requirements ... 30
5.3.2Background check procedures ... 30
5.3.3Initial training requirements ... 30
5.3.4Ongoing training requirements and frequency ... 30
5.3.5Frequency and sequence for job rotation ... 30
5.3.6Disciplinary measures for unauthorized actions ... 30
5.3.7Requirements with respect to third party contracting ... 30
5.3.8Documentation supplied to personnel ... 31
5.4 AUDIT LOGGING PROCEDURES ... 31
5.4.1Types of events to be recorded ... 31
5.4.2Frequency of audit log processing ... 31
5.4.3Audit log retention ... 31
5.4.4Audit log protection ... 31
5.4.5Audit log backup procedure ... 32
5.4.6Audit log collection system ... 32
5.4.7Providing notification that an event has been logged ... 32
5.4.8Vulnerability assessment ... 32
5.5 DATA ARCHIVAL ... 32
5.5.1Types of records that are archived ... 32
5.5.2Archive retention period ... 32
5.5.3Archive protection ... 32
5.5.4Requirements for time-stamping of records ... 33
5.5.5Archive collection system ... 33
5.5.6Procedures to obtain and verify archived data ... 33
5.6 KEY CHANGEOVER ... 33
5.7 COMPROMISE AND DISASTER RECOVERY ... 33
5.7.1Procedures for reporting and handling incidents and compromised events ... 33
5.7.2Recovery procedures in the event that hardware, software or data become corrupted ... 33
5.7.3Recovery procedures in the event that the private key of the CA component is compromised ... 34
5.7.4Business continuity capabilities following an incident ... 34
5.8 CA OR RA TERMINATION ... 34
6 TECHNICAL SECURITY CONTROLS ... 34
6.1 KEY PAIR GENERATION AND INSTALLATION ... 34
6.1.1Key pair generation ... 34
6.1.2Private Key delivery to holder ... 35
6.1.3Holder's Public key delivery to the CA server ... 35
6.1.4CA public key delivery to holders ... 35
6.1.5Key size ... 35
The "Banka Slovenije Root CA" server uses a 4,096 bit RSA private key to sign, while the "Banka Slovenije Ent Sub CA" server uses a 2,048 bit RSA private key to sign. ... 35
6.1.6Key pair parameter generation ... 35
6.1.7Key usage purposes (defined in X.509 v3 fields "key usage" and "extended key usage") ... 35
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 36
6.2.1Cryptographic module standards ... 36
6.2.2Private Key multi-person (n out of m) control ... 36
6.2.3Private Key Escrow ... 36
6.2.4Private Key Backup ... 36
6.2.5Private Key Archive ... 37
6.2.6Private Key transfer to cryptographic module ... 37
6.2.7Private Key storage in a Cryptographic Module ... 38
6.2.8Private Key activation method ... 38
6.2.9Private Key deactivation method ... 38
6.2.10 Private Key destruction method ... 38
6.2.11 Cryptographic Module Capabilities ... 38
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT ... 38
6.3.1Public key archiving ... 38

6.3.2Operational period of issued digital certificates ... 38
6.4 ACTIVATION DATA ... 39
6.4.1Generation and installation of activation data ... 39
6.4.2Activation Data protection ... 39
6.4.3Other aspects of activation data ... 39
6.5 COMPUTER SECURITY CONTROLS ... 39
6.5.1Specific security technical requirements ... 39
6.5.2Computer system security rating ... 39
6.6 LIFECYCLE SECURITY CONTROLS ... 40
6.6.1System development controls ... 40
6.6.2Security management controls ... 40
6.7 NETWORK SECURITY CONTROLS ... 40
6.8 TIME-STAMPING ... 40

7 CERTIFICATE AND CRL PROFILES ... 40

7.1 CERTIFICATE PROFILES ... 41
7.1.1Version number ... 41
7.1.2Certificate extensions ... 41
7.1.3Algorithm Object Identifiers (OID) ... 42
7.1.4Name formats ... 42
7.1.5Name constraints ... 42
7.1.6Certificate Policy Object Identifiers (OID) ... 42
7.1.7Use of the "Policy Constraints" extension ... 42
7.1.8Syntax and semantics of the "Policy qualifiers" ... 42
7.1.9Processing semantics of the critical "Certificate Policy" extension ... 42
7.2 CRL PROFILE ... 42
7.2.1Version number ... 42
7.2.2CRL and extensions ... 43
7.3 OCSP PROFILE ... 43

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT ... 43

8.1 FREQUENCY OF COMPLIANCE AUDIT AND OTHER ASSESSMENT ... 43
8.2 IDENTITY AND QUALIFICATIONS OF AUDITORS AND ASSESSORS ... 43
8.3 THE RELATIONSHIP BETWEEN THE ASSESSOR AND THE ENTITY BEING ASSESSED ... 43
8.4 SCOPE OF AUDITS AND ASSESSMENTS ... 43
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCIES ... 43
8.6 NOTIFICATION OF THE RESULTS ... 44

9 OTHER BUSINESS AND LEGAL MATTERS ... 44

9.1 FEES ... 44
9.2 FINANCIAL RESPONSIBILITY ... 44
9.2.1Insurance ... 44
9.2.2Other Assets ... 44
9.2.3Insurance or warranty coverage for holders ... 44
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION ... 44
9.3.1The scope of Confidential Information ... 44
9.3.2Information not within the scope of confidential information ... 44
9.3.3Responsibility to protect confidential information ... 44
9.4 PRIVACY OF PERSONAL INFORMATION ... 45
9.4.1Personal information protection plan ... 45
9.4.2Protected personal information ... 45
9.4.3Information not deemed personal ... 45
9.4.4Responsibility to protect personal information ... 45
9.4.5Notice and consent to use personal information ... 45
9.4.6Disclosure of personal information ... 45
9.4.7Other circumstances to disclose personal information ... 45
9.5 INTELLECTUAL PROPERTY RIGHTS ... 45

9.6 REPRESENTATIONS AND WARRANTIES 45
9.6.1 Obligations of the CA 45
9.6.2 Obligations of the RA 46
9.6.3 Obligations of certificate holders 46
9.6.4 Obligations of relying parties 46
9.7 DISCLAIMERS OF WARRANTIES 46
9.8 LIMITATIONS OF LIABILITY 46
9.9 INDEMNITIES 46
9.10 TERM AND TERMINATION 46
9.10.1 Term 46
9.10.2 Termination 46
9.10.3 Consequences of the termination 46
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 47
9.12 AMENDMENTS 47
9.12.1 Amendment procedures 47
9.12.2 Notification period and mechanism 47
9.12.3 Circumstances in which the OID must be changed 47
9.13 DISPUTE RESOLUTION PROCEDURES 47
9.14 VALID LEGISLATION 47
9.15 COMPLIANCE WITH APPLICABLE LAW 47
9.16 MISCELLANEOUS PROVISIONS 47
9.16.1 Entire agreement clause 47
9.16.2 Transfer of operations 47
9.16.3 Severability clause 48
9.16.4 Receivables 48
9.16.5 Force majeure 48
9.17 OTHER STIPULATIONS 48

Pursuant to the Article 1.3.2 of the CERTIFICATION AUTHORITY AT THE BANK OF SLOVENIA CERTIFICATE POLICY for digital certificates for individuals, I hereby issue the following

1 Introduction

The Certification Authority (CA) at the Bank of Slovenia (BS) issues digital certificates for which the highest level of security applies, and acts in accordance with the European System of Central Banks (ESCB) Certificate Acceptance Framework and other applicable regulations and recommendations.

The Certificate Practice Statement (CPS) defines the procedures carried out by the CA to manage the lifecycle of digital certificates including application requests, issuances, expirations or revocations. This document also defines the procedures performed by the CA to manage the corresponding infrastructure.

The CPS is compliant with all the Certificate Policies (CP) to which it is referred in Appendix 1 – References to other documents of the Bank of Slovenia

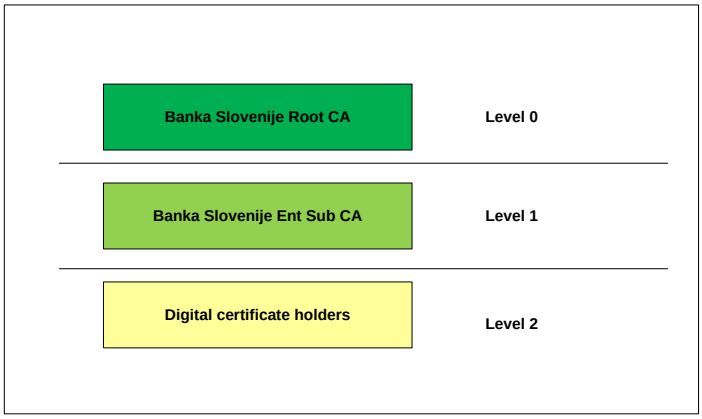
In accordance with the Bank of Slovenia confidentiality classification scheme this document is defined as "Public document", and is made publicly available on the Bank of Slovenia website.

The CP has been structured in accordance with the guidelines contained in the reference document RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" (version approved in November 2003), which was defined by the PKIX working group in the IETF (Internet Engineering Task Force). All the sections stated in RFC 3674 were included, so this CP can be easily compared with the CP documents of other certification authorities. Those sections where no special rules were defined are marked as "no stipulation".

1.1 Infrastructure of the CA at the BS

The infrastructure of the CA at the BS is managed by the Information Technology department (IT) at the BS.

The CA infrastructure is composed of two hierarchically related CA servers as shown in picture 1:



Picture 1: CA infrastructure at the BS

The highest rank in the hierarchy is "**Banka Slovenije Root CA**" which issues digital certificates to subordinate CAs.

The subordinate "**Banka Slovenije Ent Sub CA**" issues digital certificates to individuals and for the systems used by the CA to manage the digital certificates and BS identity cards (ID cards) of certificate holders.

1.2 Document name and identification

The full name of this document is "CERTIFICATION PRACTICES STATEMENT OF THE CERTIFICATION AUTHORITY AT THE BANK OF SLOVENIA"

Object Identification (OID) of the document is: **1.3.6.1.4.1.27213.2.2.1.2.1.2**

The CPS is compliant with the requirements for digital certificates issued under the following policies:

Digital certificate name	Issuance OID	Policy name and OID
Package of advanced digital certificates issued on the BS ID card.	1.3.6.1.4.1.27213.2.1.1.1.1.2 1.3.6.1.4.1.27213.2.1.1.1.2.2 1.3.6.1.4.1.27213.2.1.1.1.3.2	Certificate policy for digital certificates for individuals (OID 1.3.6.1.4.1.27213.2.2.1.1.1.2)
CA infrastructure digital certificates	1.3.6.1.4.1.27213.2.1.1.10.1.1 1.3.6.1.4.1.27213.2.1.1.8.1.1 1.3.6.1.4.1.27213.2.1.1.8.1.1 1.3.6.1.4.1.27213.2.1.1.9.1.1 1.3.6.1.4.1.27213.2.1.1.1.3.1	The certificates issued are specified in section 7.1.

1.3 PKI participants

Refer to the corresponding CP for the certificate issued.

1.3.1 Certification Authority at the BS

The CA is established at the BS, which issues digital certificates in accordance with the applicable regulations and recommendations.

1.3.2 The Policy Approval Authority

Refer to the corresponding CP for the certificate issued.

1.3.3 Certification Authority servers

The CA servers run on the Windows operating system with Microsoft CA services.

The CA server private keys are protected with hardware security modules (HSM). Private keys stored on the HSM are managed by the vendor management software . Access to the HSM is granted to HSM Administrator Card Set operators (ACS) and to HSM Operator Card Set operators (OCS), as defined in the document "CA Key Generation Ceremony in Banka Slovenije". In order to activate and use the Banka Slovenije Root CA private key, multi-person (2 out of the 6) control needs to be established. In order to activate and use the Banka Slovenije Ent SUB CA, at least 1 of the 6 OCS operators is required. All accesses are controlled following the four eyes principle.

1.3.4 Registration Authority

The RA consists of the following:
- A helpdesk operated by the BS IT department. The Helpdesk receives applications for digital certificates and verifies the identity of applicants during certificate re-key, revocation or suspension.
- The BS Reception Service, which is operated by the BS Building Services department. The BS Reception Service verifies the identity of applicants during acceptance of the BS ID card containing digital certificates.

In the course of its duties, the RA uses the following software and applications:
- Card Management System (CMS) for the BS ID cards

  Users must logon to the CMS using the advanced digital certificate stored on the BS ID card and protected with a PIN. The system is used to manage the lifecycle of the BS ID cards, including initial personalization and management of the certificates stored on the card.

- Internal records of BS personnel and contractors

  - The BS Address Book is published on the intranet.

    Users must logon using the advanced digital certificate stored on the BS ID card. Searches for the following information may be carried out by using the address book: first name, surname and photo.

- Employee and contractor register in Oracle

  Users must logon using the advanced digital certificate stored on the BS ID card and protected with a PIN. Searches for the following information may be carried out by using the register: first name, surname and personal BS ID number.

1.3.5 Key Archive

The Key Recovery Officers (KRO) are:
- The Assistant Directors of the BS IT department

The KRO must logon to the CMS by using the advanced digital certificate stored on the BS ID card and protected with a PIN.

Requests to access the Key Archive Service are defined in the CP for the digital certificate issued.

1.3.6 Digital certificate users

Refer to the corresponding CP for the certificate issued.

1.3.6.1 Digital certificate holders

Refer to the corresponding CP for the certificate issued.

1.3.6.2 Relying parties

Refer to the corresponding CP for the certificate issued.

1.4 Certificate usage

Refer to the corresponding CP for the certificate issued.

1.4.1 Appropriate certificate use

Refer to the corresponding CP for the certificate issued.

1.4.2 Prohibited use of certificates

Refer to the corresponding CP for the certificate issued.

1.5 Policy administration

The CPS must be revised at least once a year.

1.5.1 Contact information

The Chief Information Security Officer (CISO) is the contact person responsible for managing the CP, and is also the recipient of related messages and questions sent to the contact address published in the CP.

The Assistant Director of the BS IT department is the contact person responsible for managing the CPS.

1.5.2 Procedures to change the CP and the CPS

The responsible contact person for managing the CP in accordance with at least the required frequency of reviewing the document, as specified by the CP verifies any change requests for mutual recognition within the Certificate Acceptance Framework (CAF) of the European System of Central Banks (ESCB), technological changes or changes to business requirements. On the basis of the changes detected, the necessary amendments to the CP are carried forward and communicated with the responsible contact person for managing the CPS.

The responsible contact person for managing the CPS based on modified policy requirements, prepares proposals for necessary changes to the CPS and presents them to the management of the IT department.
The IT department verifies the need for any infrastructural changes to enable the implementation of the modified CP and CPS and informs the responsible contact person for managing the CP of the estimated implementation deadline by which it will provide the required infrastructure changes.

The responsible contact person sends the change proposal, implementation deadline and cost estimation to the Policy Approval Authority defined in section 1.3.2 for approval.

After the proposed changes have been approved, the BS IT department begins implementation and informs the responsible contact person for managing the CP when the change has been executed.

The responsible contact person for managing the CPS submits proposed changes to the CPS to the responsible person for managing the CP for confirmation of compliance with the CP.

1.5.3 Person responsible for determining CPS compliance with the CP

Defined in the CP under which the digital certificates were issued.

1.5.4 Publishing the policy

All amendments and changes, including a copy of this document, will be published on the BS interenet at URL: http://ca.bsi.si/pki.

1.6 Definitions and Acronyms

The terminology used in this document is defined in the corresponding CP.

The table below defines the acronyms used that are specific to the BS.

Acronym	Meaning
IT	Information Technology Department at the Bank of Slovenia
HR	Human Resources Department at the Bank of Slovenia
GS	General Services Department at the Bank of Slovenia

2 Publication and Repository Responsibilities

Publicly available data are published on the web portal owned and operated by the BS at URL (http://www.bsi.si).

The register of publicly published information end records is defined in the corresponding CP.

2.1.1 Frequency of publication

The frequency and date of publication are defined in the corresponding CP.

2.1.2 Access control on published information

Publicly published information is accessible to all website visitors.

Access permissions are used to protect publicly published information against unauthorized modification or deletion.

Each publication must be approved by authorized BS personnel.

Publications are performed by authorized BS personnel, who must logon with the advanced digital certificate stored on the BS ID card and protected with a PIN.

3 Identification and Authentication

3.1 Naming

3.1.1 Name types

Name types are in compliance with the corresponding CP.

The base register for holder identification data is the BS human resources database, where the data entered is based on the nationally recognized identity document.

3.1.2 The need for names to be meaningful

Refer to the corresponding CP for the certificate issued.

3.1.3 Use of anonymous names and pseudonyms

Refer to the corresponding CP for the certificate issued.

3.1.4 Rules for interpreting various name forms

The rules for interpreting various name forms are defined in the CP.

3.1.5 Uniqueness of names

The "subject" field contained in the digital certificate must be unique.

Uniqueness is guaranteed with the serial number contained in "Subject" field. The serial number is a 12 digit number structured by the following rules:

Serial number digit	Meaning	Value
1-2	Type of certificate	00–99
3	Tip of holder 1=employee 2=contractor 3=scholarship 4=practitioner 5=student services 6=award winners 7=scholarship abroad	0–9
4-9	Holder ID (unique random 6 digit number)	000000–999999
10-11	Reserved for future use	00–99 (currently 00)

Serial number digit	Meaning	Value
12	Control code	0–9

Cross checking controls are used in the HR database so as to ensure that the serial number is unique.

3.1.6 Name dispute resolution procedures

Defined in the corresponding CP.

3.1.7 Recognition, authentication and the role of trademarks

3.2 Refer to the corresponding CP for the certificate issued.Initial identity validation

All applications for digital certificate should be addressed to the RA, who will in turn verify the authenticity of the data contained in the application with the data contained in the recognized identity document.

3.2.1 Method to prove possession of a private key

The method that needs to be followed in order to prove possession of the private key is defined in the corresponding CP.

To prove the possession of a private key and its relation to the public key PKCS#10 request is used in accordance with the RSA PKCS#10 Certificate Request Syntax Standard.

3.2.2 Validation of the organization’s identity

Defined in the corresponding CP.

3.2.3 Validation of an individual identity

During acceptance of the BS ID card, applicants must show their ID.

In the verification process conducted by a security guard at the BS reception, in addition to verification of the identity and validity of the official personal document, it should also be checked whether the data in the application for the digital certificate matches the data in the personal document.

3.2.4 Non-verified applicant information

Please refer to the corresponding CP for the certificate issued.

3.2.5 Validation of authority

The RA verifies whether application requests have been properly approved:
- applications for BS personnel must be approved by the HR department
- applications for contractors must be approved by the manager of the BS department who proposed that a contract with the applicant be signed.

The RA verifies the authenticity of signatories following the rules defined in the documents " Resolution on Signing Authority for the Bank of Slovenia" and "Rules on organization of the Bank of Slovenia".

A digital certificate re-key is carried out on the basis of the signed written request of the holder.

3.2.6 External CA interoperation

The minimum criteria when considering the suitability of an external CA to interoperate with the CA are as follows:
- the external CA must be one of the public CAs accredited in the Republic of Slovenia
- the external CA must be authorized by the ESCB Information Technology Committee (ITC) for compliance with the ESCB Certificate Acceptance Framework (CAF)

3.3 Identification and Authentication for re-key requests

During re-key of a digital certificate, the holder must come to the helpdesk premises and produce a valid BS personal ID card.

The RA at the helpdesk must verify the following data:
- first name and surname
- BS ID number
- photo

If the holder does not have a BS ID card, the procedure is the same as for initial registration.

3.4 Identification and authentication for revocation requests

The RA verifies the identity of the requester for certificate revocation in the same manner as for certificate applications.

Revocation requests the holder send and digitally sign with own digital certificate that can be used for digital signature are not additionally verified.

The RA verifies the authenticity of signatories following the rules defined in the documents "Resolution on Signing Authority for the Bank of Slovenia" and "Rules on organization of the Bank of Slovenia".

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The digital certificate application form is published on the CA website at the URL defined in section 2.

4.1.1 Who can submit a certificate application

Please refer to the corresponding CP for the certificate issued.

4.1.2 Preparing applications and applicant's responsibilities

Certificate applications for BS personnel must be sent by the BS Human Resources department.

Certificate applications for contractors must be sent by the manager of the BS department who proposed that a contract with the applicant be signed.

Applications for re-key requests may be sent by the certificate holder itself.

Completed and signed applications shall be sent to the RA at the helpdesk.

4.2 Certificate Application Processing

4.2.1 Performing the identification and authentication procedure

All applications for digital certificates issued by the CA are processed by the RA at the helpdesk.

Processing is carried out as follows:
- the RA verifies that the data in the application is compliant with the data in the BS human resources database. The following data shall be checked: first name, surname and BS ID number and unique identification number;[1]

[1] personal identification number (EMŠO; for Slovenian nationals), or comparable national identification number (for foreign nationals).

- if the holder has no ID card or requires a new one, the RA initiates the process of printing a new ID card for the holder
- the RA verifies that the application and the statement of acceptance defined in section 4.4 are complete and include all the data to be contained in the digital certificates issued (first name, surname, organization, e-mail, serial number)
- the RA through the CMS software trigger automated process for: personalization of ID card for the holder, generating a key pair for each digital certificate and their safe storage on the ID card, preparation and submission of the certificate issue request to the CA, generating a PIN and PUK to protect access to the private keys stored on the ID card, to issue digital certificates and store them on the ID card
- the RA at the helpdesk shall send the issued ID card to the RA at reception, and the ID card activation data (PIN) to the holder's department secretary
- the RA shall safely store all the documentation received by the application for digital certificates

4.2.2 Approval or rejection of digital certificate applications

Please refer to the corresponding CP for the certificate issued.

4.2.3 Processing time

Please refer to the corresponding CP for the certificate issued.

4.3 Certificate Issuance

4.3.1 Actions performed by the CA during the issuance

The following actions are performed by the CA:
- the authorised RA person shall logon to the CMS
- the authorised RA person shall search for the holder record by using its name, surname, the BS ID number
- the authorised RA person shall approve the issuance of a package of digital certificates for the holder
- the CMS software initiates a process of key pair generation for each digital certificate
- the CMS software prepares a PKCS#10 request for each digital certificate and forwards it to the CA server

Upon receiving the request, the CA server performs the activities below:
- verifies the identity of the CMS
- verifies the validity of the PKCS#10 request
- issues a digital certificate for the received PKCS#10 request
- returns the digital certificate issued to the CMS

4.3.2 Notification mechanisms used by the CA to notify the holder

Please refer to the corresponding CP for the certificate issued.

4.4 Certificate Acceptance

4.4.1 Procedure for accepting the certificate

Please refer to the corresponding CP for the certificate issued.

4.4.2 Publication of the certificate

Please refer to the corresponding CP for the certificate issued.

4.4.3 Notification of certificate issuance by the CA to other entities

Please refer to the corresponding CP for the certificate issued.

4.5 Key Pair and Certificate Usage

4.5.1 Holder's use of the private key and the digital certificate

Please refer to the corresponding CP for the certificate issued.

4.5.2 Relying party use of the public key and the digital certificate

Please refer to the corresponding CP for the certificate issued.

4.6 Certificate Renewal

Please refer to the corresponding CP for the certificate issued.

4.7 Certificate re-key

4.7.1 Circumstances for certificate re-key

Please refer to the corresponding CP for the certificate issued.

4.7.2 Who may request certificate re-key?

Please refer to the corresponding CP for the certificate issued.

4.7.3 Procedure for processing certificate re-key

The RA at the helpdesk verifies that the application has been completed and signed by holder.

The RA verifies the identity of the holder by checking the following:
- that the data contained in the application matches the data in the human resources database and matches the data contained in the holder's existing BS ID card
- that the person bearing the ID card corresponds with the photo printed on the ID card

4.7.4 Notification of re-key to the certificate holder

Please refer to the corresponding CP for the certificate issued.

4.7.5 Acceptance of the certificate

Please refer to the corresponding CP for the certificate issued.

4.7.6 Publication of issued certificate after certificate re-key

Please refer to the corresponding CP for the certificate issued.

4.7.7 Notification of certificate issuance by the CA to relying parties

Please refer to the corresponding CP for the certificate issued.

4.8 Certificate Modification

Please refer to the corresponding CP for the certificate issued.

4.9 Revocation and suspension of digital certificate

4.9.1 Grounds for revocation

Please refer to the corresponding CP for the certificate issued.

4.9.2 Who can request certificate revocation

Please refer to the corresponding CP for the certificate issued.

4.9.3 Procedure used for certificate revocation request

Please refer to the corresponding CP for the certificate issued.

Standard procedure:

The personnel of the CA revoke the digital certificate according to the procedure set out in the policy.

Extraordinary procedure:

After receiving a telephone call requesting the revocation of a digital certificate, the security guard at BS reception:
- records the first name and surname of the holder of the digital certificate and the caller's telephone number;
- in a procedure coordinated with the IT department, calls the IT contact persons on the Help for Users call list;
- transfers the recorded data for the revocation of the digital certificate to the first contact that answers the call.

The IT contact person suspends the digital certificate according to the procedure defined in the policy.

4.9.4 Grace period available to holder to prepare the revocation request

Please refer to the corresponding CP for the certificate issued.

4.9.5 The time within which the CA should process revocation requests

4.9.5.1 Digital certificates of holders

Please refer to the corresponding CP for the certificate issued.

4.9.5.2 Digital certificates of the CA

Revocation of the digital certificate used by the CA to digitally sign issued digital certificates must be carried out immediately.

4.9.6 Revocation checking requirements for relying parties

Please refer to the corresponding CP for the certificate issued.

4.9.7 The CRL issuance frequency

Please refer to the corresponding CP for the certificate issued.

4.9.8 Maximum latency between the generation of CRLs and their publication

Please refer to the corresponding CP for the certificate issued.

4.9.9 Online certificate revocation status checking

Please refer to the corresponding CP for the certificate issued.

4.9.10 Online revocation checking requirements

Please refer to the corresponding CP for the certificate issued.

4.9.11 Other forms of revocation alerts available

Please refer to the corresponding CP for the certificate issued.

4.9.12 Special requirements for the revocation of compromised keys

In the event that the CA digital certificate must be revoked due to abuse of the private key, the BS Public Relation services shall prepare a short press release and publish it on the CA website.

4.9.13 Grounds for suspension of a digital certificate

Please refer to the corresponding CP for the certificate issued.

4.9.14 Who can request or cancel the suspension of a digital certificate

Please refer to the corresponding CP for the certificate issued.

4.9.15 Procedure for suspension of a digital certificate

Please refer to the corresponding CP for the certificate issued.

4.9.16 Duration of suspension of a digital certificate

Please refer to the corresponding CP for the certificate issued.

4.10 Certificate Status Services

4.10.1 Operational characteristics

Please refer to the corresponding CP for the certificate issued.

4.10.2 Service availability

The CA ensures high availability by continuously monitoring the system, with regular maintenance, by component and path duplication, with business continuity plans and

by creating a backup computer center. A description of the mechanisms used and processes carried out by the CA is detailed in the BS business continuity plans. In accordance with the confidentiality classification scheme used in the BS, documents are classified as "*Confidential*" and are accessible only to authorized personnel on a "need to know" basis.

4.10.3 Additional features

Please refer to the corresponding CP for the certificate issued.

4.11 Termination of the relationship between the holder and the CA

Please refer to the corresponding CP for the certificate issued.

4.12 Key Escrow and Recovery

4.12.1 Key archive and recovery policies

Please refer to the corresponding CP for the certificate issued.

4.12.1.1 Key recovery procedure

Key recovery shall be carried out as follows:

- the holder sends a key recovery request to the RA
- the holder comes to the RA premises with his or her personal BS ID card
- the RA verifies the identity of the holder (first name, surname, BS ID number and photo) and, by using the CMS, initiates the key recovery process which takes place in the following order:
    1. the CMS generates an import RSA key pair on the ID card where the encryption key must be inserted
    2. the CMS sends the public key for the import RSA key pair to the CMS Remote Key Manager service (RKM) and requests that a recoverable key be generated by the RKM
    3. the RKM generates an extractable RSA key pair and symmetric session key on the HSM
    4. the RKM extracts the private key for the extractable RSA key pair using the AES session key. The private key only leaves the HSM when encrypted by the session key
    5. the RKM extracts the symmetric session key using the public key for the import RSA key pair. The session key only leaves the HSM when encrypted by the public key for the import RSA key pair,
    6. the RKM sends the encrypted private key and encrypted session key to the CMS,
    7. the CMS inserts the symmetric session key and private key on the token,
    8. the CMS server removes the import key pair from the token.

4.12.1.2 Key disclosure procedure

Key disclosure shall be carried out as follows:
- the RA receives a request to disclose the private key of a holder
- the RA validates and verifies the request and, if appropriate, notifies 1 out of the 2 Key Recover Officers (KRO) at the BS
- the RA prepares a blank ID card which will be used to recover and store the private key
- by using the CMS, the RA initiates a request to disclose the private key
- the KRO comes to the RA premises at the helpdesk and verifies the suitability of the approval for the request
- the KRO inserts its own BS ID card into the card reader in order to approve the request
- the CMS software performs blank ID card personalization on the name of the holder
- the CMS performs actions 1, 2 and 3 as defined in section 4.12.11 (Key recovery procedure)

4.12.2 Session key protection

The transport key used to transfer the private key is protected with encryption by the temporary RSA import key pair that is generated on the cryptographic token of the BS ID card. This process is detailed in section 4.12.1.1.

5 Management, Operational and Physical controls

5.1 Physical security controls

In this section only the most significant controls that are implemented are described. A more detailed description is provided in the BS internal documents in the field of physical protection.

5.1.1 Site location and construction

The BS buildings and premises are physically secured.

The CA server equipment is installed in the BS main and disaster computing centres, which have the following controls provided:
- the rooms are without windows
- physical access control and individual transitions
- surveillance cameras at the entrances and on the premises
- the rooms are equipped with fire, water leakage and movement detectors
- there are three security zones. Transitions between zones are physically separated and secured by additional physical access control
- the wiring is separated for power and communication and is carried out according to specific channels

5.1.2 Physical access

Only BS personnel can enter the Bank of Slovenia buildings. Visitor arrivals must be announced in advance and approved. All visitors shall be escorted by a BS employee.

To enter the building, it is necessary to register with the BS ID card.

Only authorized personnel in the IT department can enter the computing center premises. It is necessary to register with the BS ID card before entering the computing center premises.

To move between the security zones it is necessary to register with the BS ID card and enter a PIN code.

Access rights to individual zones are assigned on a "need to know" basis.

5.1.3 Power and air conditioning

The BS computing center is connected to the mains via an Uninterruptable Power Supply (UPS) which, in the event of failure, ensures the autonomy of the computing center for at least 45 minutes. In order to ensure a longer period of autonomy, a diesel unit is automatically switched on.

The equipment connected to the BS computing center premises has two separate power adapters.

The computing center premises are air-conditioned and maintain the temperature in accordance with the manufacturers' specifications for the normal operation of the equipment. The cooling load is evenly distributed over two air conditioners. In the event of a failure of one air conditioner, the other device's capacity ensures that the correct temperature is maintained.

5.1.4 Water exposures

The equipment and wiring are adequately protected against water leakage.

5.1.5 Fire prevention and protection

All the rooms in the building are equipped with detectors and fire alarms. The alarms are routed to the physical security operations center of the BS, where 24-hour monitoring status is ensured.

The corridors and rooms of the computer center are equipped with fire extinguishers.

The CA personnel are regularly trained on how to use the extinguishers.

5.1.6 Media storage

The central disk arrays are duplicated. The critical disks on each disk array are configured in the VRAID1 system with high availability and allow for the substitution of defective disks when the system is running without downtime.

For mission critical data, regular daily backups are performed on virtual tapes, as well as on the classic media tape once per month. One copy of the tape and virtual media tape is stored in a computer center while the second copy is located separately in the backup computer center. Backup copying is undertaken by authorised personnel at the CA.

5.1.7 Waste disposal

The premises are equipped with paper shredders, which ensure the safe destruction of information in paper form.

Magnetic media is demagnetized prior to disposal.

5.1.8 Off-site backup

The central disk arrays are installed in different locations (the computer center and the backup computer center). Synchronous data replication over the SAN network is established between the disk arrays.

Two copies of the backups are performed, which are located in different sites.

5.2 Procedural security controls

5.2.1 The CA organizational structure and distribution of roles

The CA has established the following functional roles:

The **HSM System Administrator** is responsible for the HSM system administration. Critical activities in the HSM are secured by the ACS. In order to carry out critical activities in the module, the administrator must ensure the simultaneous presence of at least two of the six HSM Administrators with ACS card. The HSM System Administrator can also perform other tasks. The HSM System Administrator has approved physical access to the HSM.

The following are critical activities that cannot be carried out without HSM Administrators with an ACS card:
- creating a Security World
- restoring a Security World
- recovering private keys from backup to the HSM (if the key recovery was enabled)
- replacing existing ACS
- delegating FIPS 140-2 level 3 authorization activities
- passphrase recovery

As part of their duties, **HSM Administrators** verify the adequacy of authorization for activities that will be conducted by the HSM System Administrator and supervise their implementation. The HSM Administrator can also perform other tasks. HSM Administrators have escorted access to the HSM and do not have access to sensitive data unless they have access in combination with other roles they perform.

The HSM operator function is established for the use of OCS cards. The CA has three sets of OCS cards. Two sets are used to access the private key of the CA server. In order to access the private key of the "Banka Slovenije Root CA" server, at least two of the six HSM operators with an OCS card must be simultaneously present. To access the private key of the "Banka Slovenije Ent Sub CA" server, one of the six operators with an OCS card is sufficient. The third OCS is used to access the private key of the CMS where one of the HSM operators with an OCS card is sufficient to activate the private key. As part of their assignments, the HSM operators review the adequacy of authorization for the activities that will be carried out and controlled by the server administrators, and supervise the activities to ensure they are carried out according to the procedure prescribed in order to ensure that the audit trail has been logged adequately. The HSM operator can also perform other tasks. The HSM operator has access to the HSM.

Crypto Custodian (CC) is responsible for envelopes where the PIN codes of the ACS and OCS cards for the HSM are stored. The crypto custodian cannot perform other tasks and has no access to the HSM.

The **CA template admin (TA)** has access to the digital certificate templates stored in the Active Directory (AD). This role is accessible via a special AD username required to authenticate using a digital certificate stored on a crypto module of the BS ID card protected with a PIN. The four eyes principle is established for the use of this ID card. Access to the ID card is restricted to IT security officers, whereas the PIN code is known only to system administrators. The CA template admin can also perform other tasks. CA template admins have no access to the HSM unless access is given in combination with other roles they perform.

The **system administrator of the CA server** has permission to install, configure, maintain and shutdown the CA server software, but has no access to the CA server private key. The CA has separate system administrators for the "Banka Slovenije Root CA" server and for the "Banka Slovenije Ent Sub CA" server. System administrators can also perform other tasks. System administrators have no access to the HSM. System administrators have no access to the HSM unless access is given in combination with other roles they perform.

The **system administrator of the CMS server** has permission to install, configure, maintain and shutdown the CMS server as well as carry out basic configuration of the CMS application. However, the system administrator of the CMS server has no access to configuring workflows in the CMS application. System administrators can also perform other tasks. System administrators have no access to the HSM unless access is given in combination with other roles they perform.

In the CMS application, the **CMS application administrator** has permission to manage all the settings including access rights, workflows, and configure restoration from the backup. The CMS application administrator role is accessible via a special AD

username required to authenticate with a digital certificate stored on a crypto module of the BS ID card protected with a PIN. The four eyes principle is established for the use of this ID card. Access to the ID card is restricted to IT security officers, whereas the PIN code is known only to system administrators. CMS application administrators can also perform other tasks. CMS application administrators have no access to the HSM unless access is given in combination with other roles they perform.

The **authorizer of digital certificates for CA applications** is responsible for validating and authorizing requests to issue digital certificates used for CA software components. Authorizers can also perform other tasks. Authorizers have no access to the HSM unless access is given in combination with other roles they perform.

The **IT Security officer (SECO)** is responsible for validating the adequacy of modifications to digital certificate templates and CA software, as well as monitoring audit trails. IT security officers can also perform other tasks. IT security officers have access to the HSM unless access is given in combination with other roles they perform.

Within the scope of their duties **Key Recovery Officers (KRO)** examine the appropriateness of authorization for private key disclosure requests. KROs can also perform other tasks. KROs have access to the HSM unless access is given in combination with other roles they perform.

RA Personnel are responsible for managing the lifecycle of BS ID cards. Within the scope of their duties RA personnel approve applications for digital certificates, validate the identity of applicants and use the CMS application. RA personnel can also perform other tasks. RA personnel have no access to the HSM unless access is given in combination with other roles they perform.

The activities carried out by the above-mentioned roles during the initial HSM installation are documented in "CA Key Generation Ceremony in Banka Slovenije".

5.2.2 Number of individuals required per task

In order to perform the duties of HSM administrator, two out of six persons are simultaneously required.

In order to perform the duties of HSM operator, two out of six persons are simultaneously required for the "Banka Slovenije Root CA" server and one out of six persons is required for the "Banka Slovenije Ent Sub CA" server.

In order to perform the duties of KRO, one out of two persons is required. In relation to private key disclosures, one KRO and one member of the RA personnel are always simultaneously required to perform the task.

In order to perform the duties of CA template admin, one out of two IT security officers and one out of two system administrators are simultaneously required.

In order to perform the duties of CMS application administrator, one out of two IT security officers and one out of two system administrators are simultaneously required.

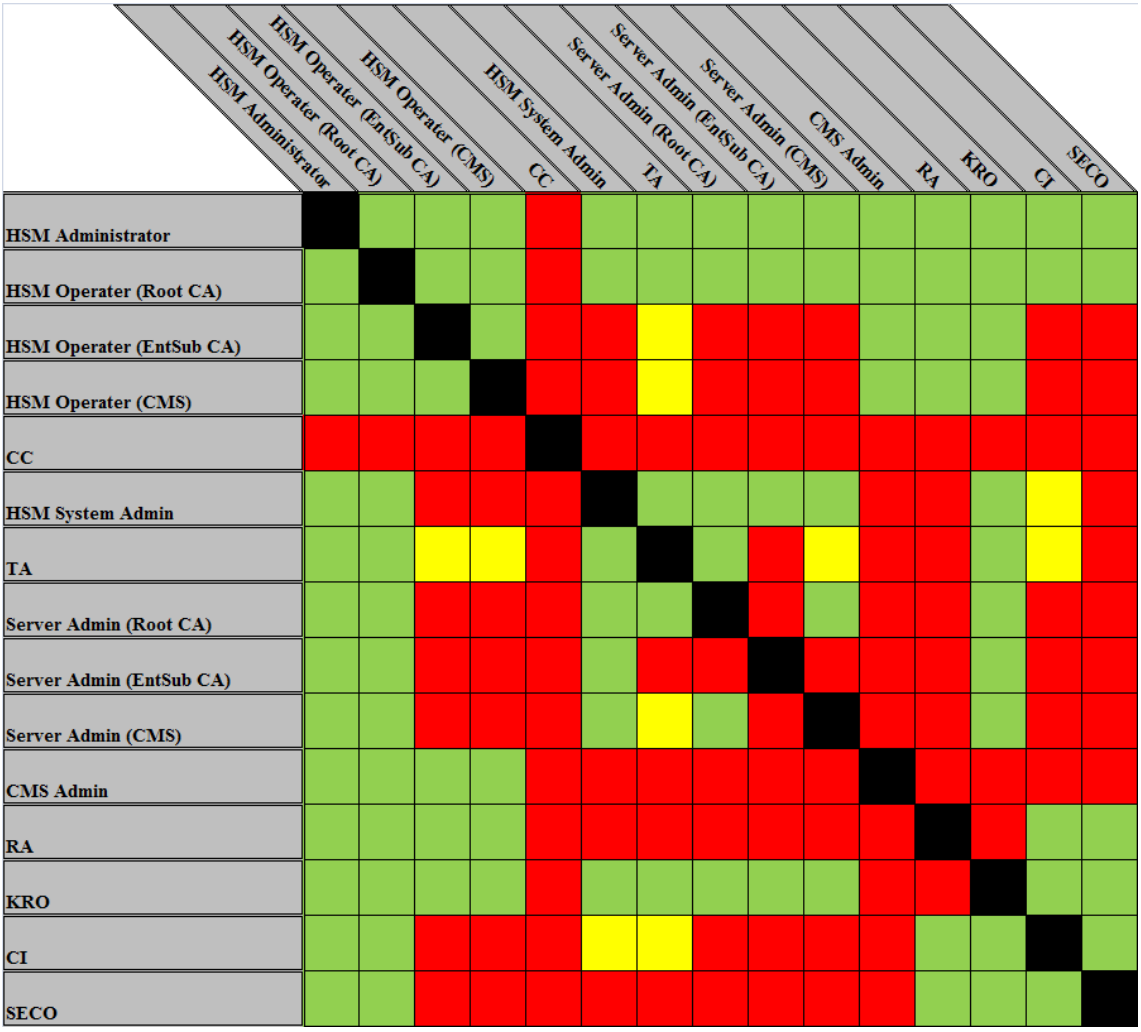
For all other tasks, the CA has defined at least two people, with one person required to perform the task.

5.2.3 Identification and authentication requirements for each role

The HSM administrators and operators are identified and authenticated in the HSM by way of shared secrecy techniques in a specific set of the HSM cryptographic cards. The card sets are generated during the initial installation of the HSM.
The rest of the CA personnel are identified by a way of digital certificates issued by the CA and authenticated by a way of cryptographic tokens.

5.2.4 Roles requiring separation of duties

Incompatible roles are provided in the following table. Red colored roles are completely incompatible with each other and may not be performed by the same person. Yellow colored tasks are, in principle, considered incompatible with each other. In order for these tasks to be carried out by the same person additional security mechanisms must be established in order to verify the authorization and traceability of the actions taken. Tasks that are colored green may be performed by the same person.



Abbreviations used in the table:
CC – Crypto Custodian
HSM System Admin – HSM System administrator
TA – Template Admin
Server Admin – Server administrator
CMS Admin – CMS application administrator
CI – Certificate issuer
SECO – IT Security officer
KRO – Key Recovery Officer
RA – The RA personnel

5.3 Personnel security controls

5.3.1 Qualifications, experience and authorization requirements

In accordance with the employment policies of the BS, the CA employs personnel with appropriate qualifications and experience.

5.3.2 Background check procedures

All candidates are verified in accordance with the law.

5.3.3 Initial training requirements

All CA personnel are regularly trained in the areas of information security and communication systems, and the specifics related to the software used by the CA and procedures carried out by the individual.

5.3.4 Ongoing training requirements and frequency

If required, depending on changes to infrastructure and personnel assignments.

5.3.5 Frequency and sequence for job rotation

"No stipulation".

5.3.6 Disciplinary measures for unauthorized actions

In the event of a violation, the Bank of Slovenia acts in accordance with the law.

5.3.7 Requirements with respect to third party contracting

CA tasks are performed without hiring outside contractors. Exceptions are made in the event of hardware failure. BS general regulations shall be applied to contracting.

5.3.8 Documentation supplied to personnel

CA personnel will be given access to the CP, the CPS and all mandatory security regulation documents in place in the BS.

5.4 Audit logging procedures

5.4.1 Types of events to be recorded

The event logging process begins at server startup, and ends at shutdown.

The following event types are recorded:
- events related to the management, archiving and use of the CA software
- events related to the holder key pairs and digital certificates (issue, acceptance, revocation, suspension)
- events related to the management and use of the CA key pairs
- events related to the preparation of smartcards for creating and storing the holder's key pair and digital certificate
- events related to the security policy and management of the operating systems and hardware
- events related to the security policy and management of the computer network
- events related to physical access to the CA premises
- events related to CA personnel changes

5.4.2 Frequency of audit log processing

Events are forwarded to the central Security Incident and Event Management System (SIEM) where alarms are set up for certain types of event that require immediate intervention.

A manual analysis of the events is performed as required.

5.4.3 Audit log retention

Information about the online retention period of audit logs on the CA servers and in the SIEM is classified as confidential and is available only to the CA personnel.

For the archive audit log retention period please refer to the corresponding CP for the certificate issued.

5.4.4 Audit log protection

Audit logs are protected on CA systems with an access rights system. Access permission is granted only to authorised personnel on a "need to know" basis.

On SIEM audit logs are automatically digitally signed by the SIEM system, which provides protection against unauthorised modification. Audit trails of the actions of the CA's security engineers who act as the administrators of the SIEM are recorded in a separate server, which is only accessible via the PAM[2] system, which ensures the traceability of any unauthorized modifications of the audit trails on the CA's servers.

5.4.5 Audit log backup procedure

Backup copies of audit logs are performed simultaneously and with the same dynamics that apply for other critical systems in the BS.

5.4.6 Audit log collection system

Audit log collection is a combination of automatic and manual processes.

Events related to the CA server logs and CMS application logs are collected automatically.

5.4.7 Providing notification that an event has been logged

"No stipulation".

5.4.8 Vulnerability assessment

A vulnerability assessment is performed in the context of the patch management process and is carried out according to the related policies in place at the BS.

5.5 Data Archival

5.5.1 Types of records that are archived

Please refer to the corresponding CP for the certificate issued.

5.5.2 Archive retention period

Please refer to the corresponding CP for the certificate issued.

5.5.3 Archive protection

Please refer to the corresponding CP for the certificate issued.

[2] Privileged Access Management

5.5.4 Requirements for time-stamping of records

Please refer to the corresponding CP for the certificate issued.

5.5.5 Archive collection system

Please refer to the corresponding CP for the certificate issued.

5.5.6 Procedures to obtain and verify archived data

Access is granted to CA authorized personnel on a "need to know" basis, as specified in section 5.2.1.

5.6 Key Changeover

The CA shall carry out the same procedures as in the initial CA private key generation. This procedure is detailed in section 6.1.1.1.

Digital certificates issued by the CA shall be published on the CA website.

On its website, the CA shall notify all participants of changes to the digital certificate.

5.7 Compromise and Disaster Recovery

5.7.1 Procedures for reporting and handling incidents and compromised events

In the event of a security incident, the CA shall proceed according to the standard procedures of the BS, as defined in the document "Guidance on the management of security incidents in the Bank of Slovenia".

5.7.2 Recovery procedures in the event that hardware, software or data become corrupted

All CA hardware is duplicated. In the event of disruption to or destruction of the main equipment, the continuation of operations is ensured through the use of back-up equipment.

In the event that the software is destroyed, the CA shall stop all systems until normal operations are restored. At the same time the CA shall initiate a procedure to discover the cause of the event and carry out any corrective actions required in order to prevent the same event from happening again.

In the event that data software is destroyed, the CA shall stop all systems until database stability is restored. If required, data will be restored from the most recent backup made.

5.7.3 Recovery procedures in the event that the private key of the CA component is compromised

If a CA's private key is compromised, the CA shall revoke all certificates signed with the compromised key, generate and publish the CRL, stop all systems and notify all holders and third parties about the event.

The CA shall re-establish operations within the shortest time possible. The CA private key shall be regenerated, as detailed in section 6.1.1.1.

5.7.4 Business continuity capabilities following an incident

The CA has duplicated production systems to remote location within the BS disaster computing center. In the event of a natural disaster which does not affect both locations, the CA shall resume operations within the timeframes expected, in accordance with the business continuity and the BS disaster recovery plans.

5.8 CA or RA Termination

Please refer to the corresponding CP for the certificate issued.

6 Technical Security controls

6.1 Key pair Generation and Installation

6.1.1 Key pair generation

6.1.1.1 The CA keys

Key pairs are generated as defined in the corresponding CP for the certificate issued.

Key pairs are stored in two HSMs. The HSM administrator with manual procedures ensures the consistency of HSM configuration and the digital certificates stored. In the event of a failure of one HSM, the other is automatically used by the CA software.

6.1.1.2 Holder keys

Please refer to the corresponding CP for the certificate issued.

6.1.2 Private Key delivery to holder

When a new BS ID card with digital certificates is issued, the holder may receive it at the reception when entering the BS building on the morning of the next business day.

When digital certificate re-key is carried out the holder immediately after issue at RA premises accepts the BS ID card with digital certificates. .

6.1.3 Holder's Public key delivery to the CA server

Public keys are transmitted between the BS ID card and the CMS in the form of a PKCS#10 formatted certificate request.

6.1.4 CA public key delivery to holders

The CA public key is transmitted to holders and relying parties in the form of an X.509 v3 digital certificate.

6.1.5 Key size

The "Banka Slovenije Root CA" server uses a 4,096 bit RSA private key to sign, while the "Banka Slovenije Ent Sub CA" server uses a 2,048 bit RSA private key to sign.

Key size of digital certificates issued to holders is defined in the corresponding CP for the certificate issued.

6.1.6 Key pair parameter generation

All procedures regarding the RSA keys are in accordance with the PKCS# 1 recommendations.

6.1.7 Key usage purposes (defined in X.509 v3 fields "key usage" and "extended key usage")

Key usage purpose is defined in the corresponding CP for the certificate issued.

All digital certificates contain an X.509 v3 "key usage" extension.

Additional constraints may be established through the "Extended key usage" extension.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

The HSM used to create the CA key pairs is FIPS 140-2 Level 3 certified.

In order to use and maintain the HSM, authorized personnel use smartcards with a cryptographic module that is FIPS 140-2 Level 3 certified.

The RA personnel use cryptographic modules on the BS ID card, which is certified as complying with CC EAL4+ security level or higher.

Holders use cryptographic modules as prescribed with the corresponding CP.

6.2.2 Private Key multi-person (n out of m) control

In order to administrate the HSM used to store the CA private keys, the CA has established a shared set of six secret smartcards with a cryptographic module to store the HSM administrator private key (ACS). Two of the HSM administrators must always login in sequence in order to carry out administrative tasks.

In order to access the "Banka Slovenije Root CA" server private key, the CA has established a shared set of six secret smartcards with a cryptographic module to store the HSM operator private key (OCS). In order to carry out tasks that require a private key, two of the HSM operators must always login in sequence.

In order to access the "Banka Slovenije Ent Sub CA" server private key, the CA has established a shared set of six secret smartcards with a cryptographic module to store the HSM operator private key (OCS). In order to carry out tasks that require a private key, at least one of the HSM operators must always login.

6.2.3 Private Key Escrow

Please refer to the corresponding CP for the certificate issued.

6.2.4 Private Key Backup

The CA private key backup

Backup copies of private keys of the CA are protected by the HSM. Backups are encrypted with the key pair stored on the OCS card.

The HSM system administrator is responsible for the private key recovery procedure, which is detailed in section 6.2.2.

The holders private key backup

Please refer to the corresponding CP for the certificate issued.

6.2.5 Private Key Archive

Archived copies of holder private keys used for encryption are encrypted with the CA private key and safely stored in the archive database. A backup of the archive database is carried out along with a backup of other CA data, as detailed in sections 5.1.6 and 5.1.8.

Recovery procedures are defined in the corresponding CP.

6.2.6 Private Key transfer to cryptographic module

The CA private keys may only be used on an activated HSM. Activation shall be carried out by the HSM system administrator, who must authenticate as detailed in 6.2.2.

The CA private keys are activated during the start-up of the CA server or start-up of the CMS application start-up. Access to the private key must be authorized by the HSM operator, who must authenticate as detailed in 6.2.2.

Holder private keys that can be used for authentication and for digital signature are generated on the cryptographic module of the BS ID card and therefore need no transfer.

A holder private key that can be used for encryption is transferred by carrying out the following procedure:

- the RA receives the application for the BS ID card for holder
- after successful verification of the identity of holder (first name, surname, BS ID number and photo), RA personnel initiate key pair generation and the issuance of a digital certificate through the CMS application, which takes place in the following sequence:
    1. the CMS generates an import RSA key pair on the ID card where the encryption key must be inserted
    2. the CMS sends the public key for the import RSA key pair to the CMS Remote Key Manager service (RKM) and requests that a key pair be generated by the RKM
    3. the RKM generates an extractable RSA key pair and symmetric session key on the HSM
    4. the RKM extracts the private key for the extractable RSA key pair using the AES session key. The private key only leaves the HSM when encrypted by the session key
    5. the RKM extracts the symmetric session key using the public key for the import RSA key pair. The session key only leaves the HSM when encrypted by the public key for the import RSA key pair,
    6. the RKM sends the encrypted private key and encrypted session key to the CMS,
    7. the CMS injects the symmetric session key and private key on the token,
    8. the CMS server removes the import key pair from the token.

6.2.7 Private Key storage in a Cryptographic Module

Specifications are provided in section 6.2.1.

6.2.8 Private Key activation method

The HSM operator is responsible for the CA private key activation. The authentication procedure carried out is detailed in section 6.2.2.

Activation procedure for private key of the holder is defined in the corresponding CP for the certificate issued.

6.2.9 Private Key deactivation method

The system administrator of the CA server is responsible for server shutdown, which deactivates the private key of the CA.

Deactivation of the private key of the holder is defined in the corresponding CP for the certificate issued.

6.2.10 Private Key destruction method

During the CA server shutdown, all data stored in RAM that is related to the private key is destroyed.

When the CA digital certificate is expired or revoked, the corresponding private key must be systematically destroyed in a non-recoverable way.

Destruction of private keys of holders is defined in the corresponding CP for the certificate issued.

6.2.11 Cryptographic Module Capabilities

Defined in section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archiving

Please refer to the corresponding CP for the certificate issued.

6.3.2 Operational period of issued digital certificates

Please refer to the corresponding CP for the certificate issued.

6.4 Activation Data

6.4.1 Generation and installation of activation data

HSM activation data is generated during the initial HSM installation. The HSM administrators and HSM operators set the PIN code for the corresponding ACS or OCS card.

The activation data for the cryptographic module on the BS ID card is generated during the initial installation and personalization of the card.

6.4.2 Activation Data protection

The HSM administrators and HSM operators write down the PIN code for their ACS or OCS card and safely store them in an envelope through which the PIN cannot be read. Smart cards and envelopes are stored separately in fireproof cabinets so that one person never has simultaneous access to two smart cards and corresponding PIN codes for cards from the same set. The procedure is described in the document "CA Key Generation Ceremony and the Bank of Slovenia".

The RA personnel shall print the PIN codes for issued BS ID cards, store them in an envelope through which the PIN cannot be read and deliver the envelope to the department secretary of the holder.

6.4.3 Other aspects of activation data

Please refer to the corresponding CP for the certificate issued.

6.5 Computer Security Controls

6.5.1 Specific security technical requirements

Some content related to this section is classified as "*confidential*" in accordance with the BS confidentiality classification scheme. It is defined in other internal acts of the CA and is accessible to authorized RA personnel on a "need to know" basis.

Specific technical security specifications are defined in the CA equipment technical security standards.

6.5.2 Computer system security rating

Some content related to this section is classified as "*confidential*" in accordance with the BS confidentiality classification scheme. It is defined in other internal acts of the CA and is accessible to RA authorized personnel on a "need to know" basis.

The CA servers are hardened in accordance with vendor and best practice recommendations.

All equipment used meets the requirements of the security policies and technical security standards that apply to BS computer systems that process data with comparable levels of confidentiality.

6.6 Lifecycle security controls

6.6.1 System development controls

Please refer to the corresponding CP for the certificate issued.

6.6.2 Security management controls

Some content related to this section is classified as "*confidential*" in accordance with the BS confidentiality classification scheme. It is defined in other internal acts of the CA and is accessible to RA authorized personnel on a "need to know" basis.

The CA has established procedures for managing incidents, problems and changes for all infrastructure components used. All changes are recorded in audit logs.

The CA has established procedures for regular monitoring the integrity of software used.

The controls implemented are specified in the CA technical security standards.

6.7 Network security controls

Some content related to this section is classified as "*confidential*" in accordance with the BS confidentiality classification scheme. It is defined in other internal acts of the CA and is accessible to RA authorized personnel on a "need to know" basis.

The CA ensures access to the computer network is limited to connections that are necessary for the use and management of the CA computer infrastructure.

The controls implemented are specified in the CA technical security standards.

6.8 Time-stamping

Please refer to the corresponding CP for the certificate issued.

7 Certificate and CRL profiles

7.1 Certificate profiles

Profiled of digital certificates of holders are defined in the corresponding CP for the certificate issued.

During the initial installation procedure, the CA issued five digital certificates needed for the operation of its computer infrastructure. For one of the digital certificates, an automatic re-key is established; the remaining four are issued in the context of a two-step verification process. The system administrator shall initiate a certificate issue request to be endorsed by the authorizer of digital certificates for CA applications.

The following types of digital certificates shall be issued:

Purpose	Private key stored in the HSM?	Validity	CA template	Automatic re-key?	OID
OCSP Response Signing	No	12 days	OCSP ResponseSigning	Yes	1.3.6.1.4.1.27213.2.1.1.10.1.1
Remote MSCA Certificate	Yes	5 years	CMS Environment User 2012	No	1.3.6.1.4.1.27213.2.1.1.8.1.1
Remote Key Manager Certificate	Yes	5 years	CMS Environment User 2012	No	1.3.6.1.4.1.27213.2.1.1.8.1.1
Enrolment Agent Certificate	Yes	5 years	BS Enrolment Agent 2012	No	1.3.6.1.4.1.27213.2.1.1.9.1.1
CMS User	No	5 years	BS CMS User 2012	No	1.3.6.1.4.1.27213.2.1.1.1.3.1

7.1.1 Version number

Please refer to the corresponding CP for the certificate issued.

7.1.2 Certificate extensions

Please refer to the corresponding CP for the certificate issued.

7.1.2.1 Standard Extensions

Please refer to the corresponding CP for the certificate issued.

7.1.3 Algorithm Object Identifiers (OID)

Please refer to the corresponding CP for the certificate issued.

7.1.4 Name formats

Please refer to the corresponding CP for the certificate issued.

7.1.5 Name constraints

Please refer to the corresponding CP for the certificate issued.

7.1.6 Certificate Policy Object Identifiers (OID)

Please refer to the corresponding CP for the certificate issued.

7.1.7 Use of the "Policy Constraints" extension

Please refer to the corresponding CP for the certificate issued.

7.1.8 Syntax and semantics of the "Policy qualifiers"

Please refer to the corresponding CP for the certificate issued.

7.1.9 Processing semantics of the critical "Certificate Policy" extension

Please refer to the corresponding CP for the certificate issued.

7.2 CRL profile

Please refer to the corresponding CP for the certificate issued.

7.2.1 Version number

Please refer to the corresponding CP for the certificate issued.

7.2.2 CRL and extensions

Please refer to the corresponding CP for the certificate issued.

7.3 OCSP profile

Please refer to the corresponding CP for the certificate issued.

8 Compliance Audit and Other Assessment

Please refer to the corresponding CP for the certificate issued.

8.1 Frequency of compliance audit and other assessment

Please refer to the corresponding CP for the certificate issued.

8.2 Identity and qualifications of auditors and assessors

Please refer to the corresponding CP for the certificate issued.

8.3 The relationship between the assessor and the entity being assessed

Please refer to the corresponding CP for the certificate issued.

8.4 Scope of audits and assessments

Please refer to the corresponding CP for the certificate issued.

8.5 Actions taken as a result of deficiencies

Please refer to the corresponding CP for the certificate issued.

8.6 Notification of the results

Please refer to the corresponding CP for the certificate issued.

9 Other Business and Legal Matters

9.1 Fees

Please refer to the corresponding CP for the certificate issued.

9.2 Financial Responsibility

9.2.1 Insurance

Please refer to the corresponding CP for the certificate issued.

9.2.2 Other Assets

Please refer to the corresponding CP for the certificate issued.

9.2.3 Insurance or warranty coverage for holders

Please refer to the corresponding CP for the certificate issued.

9.3 Confidentiality of Business Information

9.3.1 The scope of Confidential Information

Please refer to the corresponding CP for the certificate issued.

9.3.2 Information not within the scope of confidential information

Please refer to the corresponding CP for the certificate issued.

9.3.3 Responsibility to protect confidential information

Please refer to the corresponding CP for the certificate issued.

9.4 Privacy of Personal Information

9.4.1 Personal information protection plan

Please refer to the corresponding CP for the certificate issued.

9.4.2 Protected personal information

Please refer to the corresponding CP for the certificate issued.

9.4.3 Information not deemed personal

Please refer to the corresponding CP for the certificate issued.

9.4.4 Responsibility to protect personal information

Please refer to the corresponding CP for the certificate issued.

9.4.5 Notice and consent to use personal information

Please refer to the corresponding CP for the certificate issued.

9.4.6 Disclosure of personal information

Please refer to the corresponding CP for the certificate issued.

9.4.7 Other circumstances to disclose personal information

"No stipulation".

9.5 Intellectual Property Rights

Please refer to the corresponding CP for the certificate issued.

9.6 Representations and Warranties

9.6.1 Obligations of the CA

Please refer to the corresponding CP for the certificate issued.

9.6.2 Obligations of the RA

Please refer to the corresponding CP for the certificate issued.

9.6.3 Obligations of certificate holders

Please refer to the corresponding CP for the certificate issued.

9.6.4 Obligations of relying parties

Please refer to the corresponding CP for the certificate issued.

9.7 Disclaimers of Warranties

Please refer to the corresponding CP for the certificate issued.

9.8 Limitations of Liability

Please refer to the corresponding CP for the certificate issued.

9.9 Indemnities

Please refer to the corresponding CP for the certificate issued.

9.10 Term and Termination

9.10.1 Term

The term is defined in point 9.17 of the final provisions.

9.10.2 Termination

The validity of the CPS is terminated in the event that a new version of the CPS is put in force or in the event of a cessation of CA services.

9.10.3 Consequences of the termination

The obligations and constraints established under this CPS referring to audits and the protection of confidentiality shall continue to prevail following their substitution in all terms which are not contrary to those of the new version.

9.11 Individual notices and communications with participants

Please refer to the corresponding CP for the certificate issued.

9.12 Amendments

9.12.1 Amendment procedures

Please refer to the corresponding CP for the certificate issued.

9.12.2 Notification period and mechanism

Please refer to the corresponding CP for the certificate issued.

9.12.3 Circumstances in which the OID must be changed

Please refer to the corresponding CP for the certificate issued.

9.13 Dispute resolution procedures

Please refer to the corresponding CP for the certificate issued.

9.14 Valid legislation

Please refer to the corresponding CP for the certificate issued.

9.15 Compliance with Applicable Law

Please refer to the corresponding CP for the certificate issued.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement clause

Please refer to the corresponding CP for the certificate issued.

9.16.2 Transfer of operations

Please refer to the corresponding CP for the certificate issued.

9.16.3 Severability clause

Please refer to the corresponding CP for the certificate issued.

9.16.4 Receivables

Please refer to the corresponding CP for the certificate issued.

9.16.5 Force majeure

Please refer to the corresponding CP for the certificate issued.

9.17 Other stipulations

Please refer to the corresponding CP for the certificate issued.

The Certification Practices Statement enters into force on 1 January 2024.