BANKA SLOVENIJE
EVROSISTEM

RULES OF THE CERTIFICATION AUTHORITY AT THE BANK OF SLOVENIA

Public part of internal rules of the Certification Authority at the Bank of Slovenia

Type	PRV
Document ID	**PRAVILNIK-7**
Version	1
Custodian	Risk Management Department (4300)
Area	Rights, Duties, and Responsibilities of Employees
Approved by	Guvernor

»This document contains an unofficial and courtesy English translation of [Pravilnik 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.

TABLE OF CONTENTS

Pursuant to the first paragraph of Article 40 of the Bank of Slovenia Act (Official Gazette of the Republic of Slovenia, Nos. 72/06 [official consolidated version], 59/11 and 55/17), and in accordance with Article 33 of the Electronic Identification and Trust Services Act (Official Gazette of the Republic of Slovenia, No. 121/21, 189/21 – ZDU-1M and 18/23 – ZDU-1O), I hereby issue the following

1. Introduction

The Certification Authority (CA) at the Bank of Slovenia (BS) is the trust service provider which issues digital certificates for which the highest level of security applies, and acts in accordance with the eIDAS Regulation, Electronic Identification and Trust Services Act (ZEISZ), the European System of Central Banks (ESCB) Certificate Acceptance Framework and other applicable regulations and recommendations.

The Bank of Slovenia issues personal digital certificates for members of its personnel and for representatives or employees of the companies and organizations that have a contract with the Bank of Slovenia to work for the Bank of Slovenia. All the digital certificates issued under this policy, with the exception of the digital certificates for which key archiving and recovery services are provided, are issued on the hardware devices of certificate holders.

This document is the Certificate Policy (CP) and represents the public part of the internal rules of the Certification Authority at the Bank of Slovenia.

According to X.509, a certificate policy (CP) is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements". A CP may be used by a relying party to help in deciding whether a certificate, and is binding nature, are sufficiently trustworthy and otherwise appropriate for a particular application.

The CP defines the essential technical characteristics and level of security for the CA infrastructure, as well as the procedures used at the Bank of Slovenia for managing this infrastructure and the lifecycle of issued digital certificates. It contains essential provisions influencing the relationship between the CA, digital certificate holders and third parties relying on these certificates.

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".

The implementation of this CP is more precisely defined in the Certification Practices Statement of the Certification Authority at the Bank of Slovenia (CPS) document (document OID: 1.3.6.1.4.1.27213.2.2.1.2.1.3).

This document is intended to be read and consulted by all the persons and organisations that use and rely on digital certificates issued by the CA at the Bank of Slovenia, as it provides the basis to assess the level of trust they may place in these certificates.

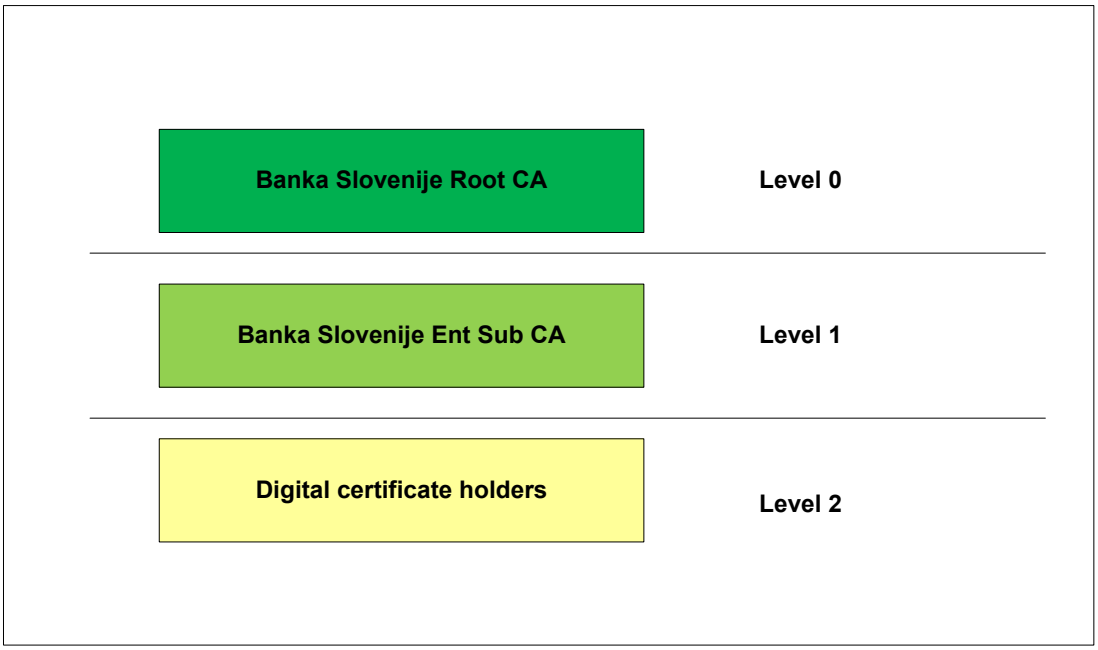
In accordance with the Bank of Slovenia confidentiality classification scheme, this document is defined as a "public document", and is made publicly available on the Bank of Slovenia website.

For further information not specified in this document interested parties may contact the persons defined in section 1.3.1.

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 Bank of Slovenia

The highest rank in the hierarchy is "**Banka Slovenije Root CA G2**" which issues digital certificates to subordinate CAs.

The subordinate "**Banka Slovenije Ent Sub CA G2**" issues digital certificates to individuals.

1.2 Document name and Identification

The name of this document is "RULES OF THE CERTIFICATION AUTHORITY AT THE BANK OF SLOVENIA".

The International Object Identification Document (OID) in accordance with ITU-T X.660 standard is: **1.3.6.1.4.1.27213.2.2.1.1.1.3**

The CP is valid for digital certificates issued under the issuance OID stated in Table 1:

Table 1: Digital certificate Issuance OIDs

Identification data	Description
Issuance OID: **1.3.6.1.4.1.27213.2.1.1.1.1.3** (ETSI QCP-n-qscd OID): 0.4.0.194112.1.2	Qualified digital certificate for electronic signature with one key pair. It is mandatory for a corresponding key pair to be generated and stored inside the cryptographic token of the BS identity card. The cryptographic token is compliant with the EAL 4+ or higher specification. A qualified digital certificate for electronic signature is issued to natural persons on a QSCD device. The qualified digital certificate can be used for qualified electronic signature and verification of digitally signed data in electronic form. The digital certificate is valid for 5 years.
Issuance OID: **1.3.6.1.4.1.27213.2.1.1.1.2.3**	A digital certificate with one key pair. It is mandatory for a corresponding key pair to be generated on the CA cryptographic module which is compliant with the FIPS 140-2 level 3 specification and stored in the CA Key Archive service that uses a cryptographic module with the same requirements. Another copy of the key pair is safely transferred and stored inside the cryptographic token of the BS identity card. Cryptographic token is compliant with the EAL 4+ or higher specification. The digital certificate can be used for encrypting and decrypting data in electronic form. The digital certificate is valid for 5 years.
Issuance OID: **1.3.6.1.4.1.27213.2.1.1.1.3.3**	A digital certificate with one key pair. It is mandatory for a corresponding key pair to be generated and stored inside the cryptographic token of BS identity card. The cryptographic token is compliant with the EAL 4+ or higher specification.

Identification data	Description
	The digital certificate can be used for authentication. The digital certificate is valid for 5 years.

1.3 PKI Participants

This section defines the entities that appear in this document.

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.

Contact data of the CA at the BS are shown below:

Address:	Bank of Slovenia Certification Authority Slovenska c. 35 1505 Ljubljana
Telephone:	+386 (1) 4719 140
Fax:	+386 (1) 2515 516
E-mail:	PKI@bsi.si
Website:	http://ca.bsi.si/pki
Centre for user support and emergency revocation:	+386 (1) 4719 111 helpdesk@bsi.si

The CA at the BS performs the following tasks:

- specifies and publishes its CP and CPS;
- specifies the application forms for its services;
- manages registers related to issued digital certificates;
- maintains an operational user support center;
- notifies its clients; and
- performs all other services in accordance with CP;

1.3.2 The Policy Approval Authority

The CP is approved by the Governor. The CPS is approved by the director of the Information Technology department.

1.3.3 Certification Authority servers

CA servers are systems that issue digital certificates and are defined in accordance with the CPS.

The following CA servers operate within the framework of the CA at the BS:

"Banka Slovenije Root CA G2" is the highest in the hierarchy of CA servers. At the beginning of its production operation the "Banka Slovenije Root CA G2" generated its own digital certificate. It issues digital certificate for its subordinate CA servers and regularly publishes its

CRL. The server is in operation only during the execution of dedicated instructions (while carrying out the operations for which it is set-up).

Holders of digital certificates issued by the "**Banka Slovenije Root CA G2"** can be solely subordinate CA servers that operate within the framework of the CA at the BS.

The most significant attributes of the "Banka Slovenije Root CA" digital certificate are as follows:

Field name	Field value:
Version	V3
Serial Number	47 5e 1d 2b ed 44 31 99 42 95 53 38 db c8 c8 49
Subject Key identifier	bf 58 0e 97 21 b8 b6 43 1a af 99 7d 4f fd aa 38 09 65 b4 f4
Issuer	CN = Banka Slovenije Root CA G2 OID.2.5.4.97=VATSI-92582087 O = Banka Slovenije C = SI
Subject	CN = Banka Slovenije Root CA OID.2.5.4.97=VATSI-92582087 O = Banka Slovenije C = SI
Valid from	15. November 2024 13:54 CET
Valid to	15. November 2054 CET
Public Key	4096 bit
Signature algorithm	sha256RSA
SHA-1 Thumbprint:	38 13 85 bd 98 a9 fe 10 36 b2 24 d6 45 d3 5b 0b cc 6b 87 d8
SHA-256 Thumbprint:	25 f4 13 79 22 f1 5f a5 5d c8 e3 c1 a6 0a 77 b1 08 d3 a3 78 75 06 b8 1a 34 22 21 fb ea 34 f0 75

"Banka Slovenije Ent Sub CA G2" is the subordinate CA server. It issues digital certificates to individuals. This CP refers to the digital certificates issued by the "Banka Slovenije Ent Sub CA G2".

Its most significant attributes are:

Field name:	Field value:
Version	V3
Serial Number	5e 00 00 00 02 60 a1 27 cf 98 a1 6b 4e 00 00 00 00 00 02
Subject Key identifier	4e 8d a8 22 5f 77 c0 7b b1 f9 4a 2b 9f ee 97 16 ce 23 0c 1d
Issuer	CN = Banka Slovenije Root CA G2 OID.2.5.4.97=VATSI-92582087 O = Banka Slovenije C = SI
Subject	CN = Banka Slovenije Ent Sub CA G2 OID.2.5.4.97=VATSI-92582087 O = Banka Slovenije

	C = SI
Valid from	15. november 2024 18:12:19 CET
Valid to	15. november 2039 18:22:19 CET
Public Key	4096 bit
Signature algorithm	sha256RSA
SHA-1 Thumbprint:	64 01 89 e3 32 87 33 6a d0 e4 1a d5 01 1a bf 03 4a c5 d9 13
SHA-256 Thumbprint:	f4 ab 52 e4 cd 2e e1 36 af 7b d5 b3 57 60 26 67 ff 29 20 11 6c 17 eb d1 d5 6f 29 41 a6 e8 9b dd

1.3.4 Registration Authority

The Registration Authority (RA) is defined in accordance with the CPS.

The RA accepts all applications regarding digital certificates issued by the CA at the BS. It verifies the identity of holders or future holders, verifies and collects necessary data in applications, submits applications to CA and maintains a register of active digital certificate holders.

1.3.5 Key Archive

Key archive is a service that provides the secure storage of copies of private keys related to digital certificates used for encryption and decryption of data in electronic form. Archived keys can be recovered only to a cryptographic token personalized for the holder of the digital certificate. Archived keys can be recovered only by authorized RA personnel. Key recovery without the presence of the digital certificate holder can only be carried out using the four eyes principle. Recovery can only be initiated by authorized RA personnel, and thereafter approved by the Key Recovery Officers.

A **Key Recovery Officer (KRO)** is an authorized individual participating during the key recovery process when the digital certificate holder is not present.

1.3.6 Digital certificate users

Digital certificate users are certificate holders and third parties.

1.3.6.1 Digital certificate holders

Digital certificate holders are individuals who are the owners of the private keys and, for this reason, stated in the "subject" field of the digital certificate. Digital certificate holders are defined in accordance with the CPS.

The CA at the BS issues digital certificates only on the basis of a formal written application. Before acceptance, all applicants must explicitly accept the terms and conditions for using the digital certificates by signing the Terms and Conditions document.

Holders of digital certificates issued by the CA at the BS can only become members of the BS personnel and representatives or employees of companies and organizations that have a contract with the BS to work for the BS (contractors).

Digital certificate holders can obtain only a package of digital certificates for individuals, stored on a cryptographic token on the BS identity card. The package contains the following:

- a qualified digital certificate for electronic signature, whose corresponding key pair is generated and stored on a cryptographic token;
- a digital certificate for encryption, whose corresponding key pair is generated on a CA cryptographic module and stored on a cryptographic token. A copy of the key pair is stored in the CA Key Archive service that uses a cryptographic module with the same requirements;
- a digital certificate for authentication, whose corresponding key pair is generated and stored on a cryptographic token;

The further liabilities of the digital certificate holder are defined in section 9.6.3.

1.3.6.2 Relying parties

Relying parties are individuals or legal persons that use digital certificates to identify the holders of digital certificates issued by the CA at the BS, or that send them encrypted data in electronic form.

For the purposes mentioned above, the relying parties must act in accordance with this CP and validate the appropriate certificate use, state and validity of the digital certificates issued by the CA at the BS.

The further liabilities of the relying parties are defined in section 9.6.4.

Relying parties may or may not be, holders of digital certificates issued by the CA at the BS, or are holders of digital certificates issued by other Certificate Authorities.

1.4 Certificate usage

Digital certificates regulated by this CP may be used within the scope of the business processes of the BS. For this purpose, digital certificates can also be used in applications within the scope of the European System of Central Banks (ESCB).

Digital certificates regulated by this policy shall be used for the purpose of electronic signature, encryption and authentication. Usage depends on the corresponding "key usage" and "extended key usage" extensions of the digital certificate, as specified in section 6.1.7.

In addition to the uses specified in the first and second paragraphs of this chapter, a qualified digital certificate for electronic signature may also be used in various commercially available applications for signing electronic documents, for the electronic signing of unilateral or mutual communications between certificate holders, and for verification of electronically signed data when the certificate holder is acting on behalf of the Bank of Slovenia.

1.4.1 Appropriate certificate use

Each digital certificate corresponds to a key pair of private and public keys.

Each digital certificate holder has three digital certificates:

- Qualified digital certificate for qualified digital signature / signature verification
  The certificate holder can use the private key to digitally sign the data in electronic form. Relying parties or the holder can use the corresponding public key to authenticate the digital signature.
- Digital certificate for encryption / decryption
  Relying parties or the holder can use the public key to encrypt the data in electronic form. The holder can use the corresponding private key to decrypt the data.
- Digital certificate for authentication
  The holder can use the key pair for authentication in computer systems operated by the BS or operated by other organizations which recognize the use of digital certificates issued by the CA at the BS.

1.4.2 Prohibited use of certificates

Digital certificates issued by the CA at the BS may be used only in accordance with applicable legislation and the rules defined in this CP, solely for the purpose specified in section 1.4.1. The BS cannot be held liable for any other type of use.

1.5 Policy administration

The CP and the CPS must be revised on a periodic basis, as specified in the CPS.

1.5.1 Contact information

The contact person for the management of the CP and the CPS can be reached at:

Banka Slovenije Overitelj digitalnih potrdil Slovenska c. 35, 1505 Ljubljana E-mail: PKI@bsi.si

1.5.2 Procedures to change the CP

The procedure for regular review of the policy is defined in the CPS.

The procedure ensures compliance with the applicable legislation and the ESCB Certificate Acceptance Framework.

The procedure ensures that the corresponding CPS and infrastructure are in line with the provisions and rules defined in the CP.

1.5.3 Person responsible for determining CPS compliance with the CP

The compliance of the CPS with the CP is reviewed by the chief information security officer.

1.5.4 Publishing the policy

Upon approval, all changes including a copy of this document must be published on the CA website at URL: http://ca.bsi.si/pki.

1.6 Definitions and Acronyms

The terminology used within the scope of this CP is as follows:

Contractors are representatives or employees of the companies and organizations that have a contract with the Bank of Slovenia to work for the Bank of Slovenia.

CPS (Certification Practices Statement) is a document that complements the CP with a detailed definition of the procedures carried out by the CA.

Digital ID (Digital Identity) is a key pair (a private key and corresponding public key) with a corresponding digital certificate issued by the CA.

Digital certificate is a certificate in electronic form, binding the data used to verify the electronic signature with the individual (certificate holder) and confirming the identity of the certificate holder. A digital certificate includes one X.509 digital certificate used by the CA to guarantee the digital identity of the certificate holder.

An **electronic signature** is a set of data in electronic form that is contained in, attached to or logically associated with other data used to verify the authenticity of that data and the identity the signer, based on a digital certificate used by the signer for signing.

Certification authority servers are systems used to issue certain types of digital certificate. The following CA server operates within the framework of the CA at the Bank of Slovenia:
- Banka Slovenije Root CA G2,
- Banka Slovenije Ent SUB CA G2

The BS ID card is a hardware device with a cryptographic token used for the secure generation and storage of key pairs and corresponding digital certificates, and is also used to perform cryptographic operations with the private keys stored.

Certificate holder (subject) is an individual stated in the "subject" certificate extension, who is the owner of the private key corresponding to the public key stated in the digital certificate.

Qualified digital certificate for electronic signature is a digital certificate issued by a trust service provider for the purpose of electronic signing, which meets the requirements set out in the eIDAS Regulation. The corresponding private key is generated and stored on a

cryptographic token, on the basis of electronic signature creation data that the signatory can, with a high level of confidence, use under their sole control, and is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Computer component refers to any software or hardware device that may be used by the CA to generate or verify electronic signatures.

Personal Identification Number (PIN) is a secret password that protects access to the cryptographic card.

Certification Authority refers to **a trust service provider** issuing certificates or performing other services related to the verification of electronic signatures and fulfilling the requirements set by the applicable legislation. In this document, the Certification Authority is the CA at the Bank of Slovenia.

Electronic signature data are unique data (e.g. encryption keys) used by the signatory to generate the electronic signature.

Electronic signature verification data are unique data (e.g. encryption keys) used to verify the electronic signature.

Signatory is the individual who generated the electronic signature.

Trust service provider is a natural or legal person that provides one or more trust services, either as a qualified or non-qualified trust service provider.

Qualified trust service provider is a trust service provider that has been granted qualified status by the supervisory authority.

Registration Authority refers to individuals or organizations responsible for collecting and managing all the data of the digital certificate holders.

Applicant refers to an individual who applies for a digital certificate him or herself.

QSCD device is a device for creating electronic signatures that complies with the requirements of the eIDAS Regulation for qualified electronic signature creation devices.

Application is a form based request to apply for or revoke a digital certificate. Forms may be accessed on the CA website (http://ca.bsi.si/PKI).

eIDAS Regulation is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Table 2: Table of acronyms

Acronym	Meaning:
AD	Active Directory
ACS	Administrator Card Set

Acronym	Meaning:
BS	Banka of Slovenia
CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
CSP	Certification Service Provider
DN	Distinguished Name
EAL	Evaluation Assurance Level
FIPS	United State Federal Information Processing Standards
HSM	Hardware Security Module
NTP	Network Time Protocol
OCS	Operator Card Set
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKIX-CMP	Public Key Infrastructure (based on) X.509 Certificate Management Protocols
RA	Registration Authority
SSCD	Secure Signature Creation Device
URL	Uniform Resource Locator

2 Publication and Repository Responsibilities

2.1 Repositories

The CA at the BS is responsible for keeping holders and relying parties promptly informed.

Publicly available data are published on the CA website at URL: http://ca.bsi.si/PKI.

Publicly accessible documents are as follows:
- the CP and the CPS
- CA servers public key data
    - Banka Slovenije Root CA G2
    - Banka Slovenije Ent Sub CA G2
- the Certificate Revocation List (CRL)
- other public data related to CA operation

The register of valid digital certificates is not publicly accessible.

The register of valid digital certificates is published in the BS Windows Active directory (AD) and contains only digital certificates used for encryption. The register is accessible only to BS Windows domain users.

2.2 Frequency of publication

The CP and the CPS are published within 24 hours of validation.

The CRLs are published as specified in sections 4.9.7 and 4.9.8.

Digital certificates used for encryption are published in AD as they are issued.

Other publicly accessible information is published as required.

2.3 Access control on published information

All publically published information may be freely accessed for reading purposes and are protected from unauthorized changes.

3 Identification and Authentication

The identity of each applicant must be validated before delivering the certificates.

Before acceptance of the BS ID card, the identity of the applicant must be verified.

3.1 Naming

Naming defines the identification data of the holder to be contained in digital certificate.

3.1.1 Types of names

Digital certificates contain distinguishing names that uniquely define the identity of the holder. Each digital certificate issued by the CA contains the following:

- Issuer distinguishing name

Field name	Distinguishing name
Issuer	CN = Banka Slovenije Ent Sub CA G2 OID.2.5.4.97=VATSI-92582087 O = Banka Slovenije C = SI

- Holder distinguishing name

Field name	Distinguishing name
Subject	CN = surname, first name Serial Number = serial number O = holder's organization C = SI

Distinguishing names are composed in accordance with the RFC 5280 and the X.501 standards.

A unique serial number is specified by the CA.

Distinguishing names may contain additional fields that are not needed to define the holder's identity.

3.1.2 The need for names to have a meaning

The distinguishing names of the certificate holder are required to have a meaning and are formed in accordance with the rules defined in section 3.1.1.

3.1.3 Use of anonymous names and pseudonyms

"No stipulation".

3.1.4 Rules for interpreting various name forms

The information contained in the distinguishing name includes letters of the English alphabet.

Other signs are converted in accordance with the rules in Table 3 below.

Table 3: Sign conversion rules

Sign	Conversion
Č	C
Š	S
Ž	Z
Ć	C
Đ	D
Ä	AE
Ö	OE
Ü	UE
Á	A
É	E
Í	I
Ó	O
Ú	U
À	A
È	E
Ì	I
Ò	O
Ù	U
Ê	E
Ô	O
Ő	O
Ű	U

All other signs are converted in accordance with the rules specified in document "ICAO Doc 9303" in the section dealing with transliteration.

3.1.5 Uniqueness of names

The assigned distinguishing names are unique for each certificate holder, and are published in the "subject" field of the certificate. The procedure used to ensure uniqueness is detailed in the CPS.

3.1.6 Name dispute resolution procedures

The name uniqueness procedures in place ensure that no name dispute situations arise.

3.1.7 Recognition, authentication and the role of trademarks

"No stipulation".

3.2 Initial identity validation

A certificate creates a bond of trust between the holder and a pair of keys contained in the certificate. The basis for this trust is the initial verification and validation of the holder's identity and evidence that the holder is in possession of a private key during the certificate issuance.

3.2.1 Method to prove possession of a private key

Key pairs are automatically generated during the personalization of the BS ID cards used to store digital certificates. Therefore no special proof of possession is envisaged. Personalization of the BS ID cards is operated by the RA.

Control of the relationship between the private and public keys and the certificate request form are standardized and detailed in the CPS.

3.2.2 Validation of the organization's identity

The CA issues digital certificates exclusively for BS personnel and contractors.

BS personnel represent the BS and so no special validation is envisaged.

Contractors represent the organizations they work for. Validation of the organization's identity is based on associated documentation provided or official records. The Bank of Slovenia department manager who initiates the contract with the external organization is responsible for ensuring the verification and validation of the organization's identity, which he or she then confirms by signing the request to issue digital certificates for the contractor. The responsible person at the BS department who initiates the contractual relationship with the external organisation is responsible for ensuring the verification of the organization's identity, and the verification of the contractual relationship between the organization and the certificate holder, which they then confirm by signing the application for the digital certificate.

3.2.3 Validation of an individual identity

Face-to-face identification is required in order to verify the identity of the digital certificate holder. The verification process is based on a nationally recognized identity document or the existing ID issued by the BS.

The following data is verified:

- First name and surname
- personal identification number (EMŠO; for Slovenian nationals), or comparable national identification number (for foreign nationals)

3.2.4 Non-verified applicant information

"No stipulation".

3.2.5 Validation of authority

The RA verifies the authority of requests related to the operation of the CA. The verification procedure is detailed in the CPS.

3.2.6 External CA interoperability

The CA at the BS can connect or recognize external CAs. A signed contact is obligatory in order to establish such a relationship.

External CAs must comply with the same or a higher level of requirements prescribed by the CA at the BS. The criteria for such interoperability are detailed in the CPS.

3.3 Identification and Authentication for re-key requests

The certificate holder must send a request to the RA for a routine key change due to key expiry or key revocation.

The process for verifying the identity of the holder is based on the existing BS ID card.

All other procedures are the same as for the initial identity validation.

3.4 Identification and authentication for revocation requests

A digital certificate revocation request may be submitted to the RA by:
- the certificate holder personally or by sending a signed revocation request form
- the holder's department manager by sending a signed revocation request form

The identity of the requester is verified by the RA. The verification procedure is detailed in the CPS.

4 Certificate Life-Cycle Operational Requirements

This section specifies the operational requirements for the life-cycle management of digital certificates issued by the CA.

4.1 Certificate Application

The CA issues certificates only on the basis of a written request.

4.1.1 Who can submit a certificate application

For BS personnel, a certificate application must be sent by the BS Human Resources department.

For contractors, a certificate application must be sent by the manager of the Bank of Slovenia department who proposed that a contract with the applicant be signed.

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

Upon receiving the application to issue the BS ID card, the CA also issues a package of digital certificates for the future holder.

4.1.2 Preparing applications and applicant's responsibilities

Digital certificate application forms are available on the CA website. Application forms must be completed, signed and sent to the RA.

The person sending the application form is obliged to validate data entered which relates to the future holder.

The holder must explicitly accept and sign the terms and conditions document before accepting the BS ID card with digital certificates.

4.2 Certificate Application Processing

4.2.1 Performing the identification and authentication procedure

The RA validates the future holder's data in the application form against the data entered in the BS human resources registers. This procedure is detailed in the CPS.

4.2.2 Approval or rejection of digital certificate applications

The RA approves or rejects certificate applications based on the criteria of completeness and validity of the data entered in the application form.

In the event that an application is rejected, the applicant is immediately notified by means of electronic mail or post.

4.2.3 Processing time

The CA shall not be held liable for any delay that may arise during the periods between applying, processing and issuing the certificate.

Normally applications will be processed and digital certificates issued within one business day.

4.3 Certificate Issuance

4.3.1 Actions performed by the CA during the issuance

The CA server issues digital certificates based on requests received from the Card Management System (CMS) of the BS.

Electronic requests between the CA server and the CMS are standardized and exchanged by secure protocols.

The CA server validates each request received for integrity and technical compliance. If no deviations are identified, the CA server issues a digital certificate and signs the certificate using the CA's private key.

This procedure is detailed in the CPS.

4.3.2 Notification mechanisms used by the CA to notify the holder

When digital certificates are issued, the CA servers do not notify holders directly.

When the BS ID card holding the certificates has been personalized and is ready to be accepted, the RA notifies the holder.

4.4 Certificate Acceptance

4.4.1 Procedure for accepting the certificate

The applicant becomes a holder of digital certificates by accepting the BS ID card holding the certificates.

The applicant must accept the BS ID card at the BS reception desk.

The reception desk officer must validate applicant's identity in accordance with the requirements stated in section 3.2.2.

Prior to accepting the BS ID card, applicants must provide a hand-written signed statement of acceptance of the terms and conditions for the use of digital certificates issued by the CA in accordance with the CP. By signing the statement, the applicants also confirm the correctness of

the personal data contained in the digital certificates issued and acceptance of the BS ID card holding the certificates.

4.4.2 Publication of the certificate

The CA publishes the issued digital certificate in the BS internal directory if publication for that type of digital certificate is prescribed by the CP.

4.4.3 Notification of certificate issuance by the CA to other entities

"No stipulation".

4.5 Key Pair and Certificate Usage

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

Holders may use their private key and the corresponding digital certificate only for the purposes authorised in section 1.4 and in accordance with the "Key Usage" and "Extended Key Usage" fields in the certificate.

Holders may use their private key and the corresponding digital certificate only if they have signed the statement of acceptance of the terms and conditions for the use of digital certificates issued by the CA in accordance with the CP.

In order to prevent the loss, disclosure, change or unauthorized use of the BS ID card, holders are obligated to physically protect the card and card activation codes as stated in section 9.6.3.

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

Relying parties may rely on the digital certificate issued by the CA only for the purposes authorized in sections 1.4 and 1.4.1.

Relying parties are obliged to verify that the digital certificates have not expired or been revoked before using them.

When using the certificates issued by the CA, relying parties are obliged to consider any other provisions set by the CP.

4.6 Certificate Renewal

Digital certificates and their corresponding key pairs have the same lifespan. Therefore at the time of renewal of the digital certificate, a renewal of the corresponding key pair is also performed.

Consequently, the remaining subsections 4.6.1 to 4.6.7 from RFC 3647 are not included in the CP and should be marked "no stipulation".

4.7 Certificate Re-key

4.7.1 Circumstances for certificate re-key

A digital certificate re-key may be due to the following:
- expiry of the existing digital certificate and the corresponding key
- change of data contained in the digital certificate
- a key pair has been compromised
- the format of the digital certificate has changed

Regular certificate re-keys can be performed during the last 30 days of validity of the existing digital certificate.

4.7.2 Who may request certificate re-key?

A certificate re-key must be requested by the certificate holder.

4.7.3 Procedure for processing certificate re-keys

The RA will verify that the holder's identification data is still valid. Any changes must be verified and registered with the formal agreement of the holder.

Renewal must be requested in person at the RA premises.

This procedure is detailed in the CPS.

4.7.4 Notification of re-key to the certificate holder

Holders must be present during certificate re-key and so no additional notification is provided by the CA.

4.7.5 Acceptance of the certificate

After certificate re-key, the holder must sign a new version of the statement of acceptance of the terms and conditions for the use of digital certificates issued by the CA in accordance with the CP.

4.7.6 Publication of issued certificate after certificate re-key

The CA publishes the digital certificate issued in the BS internal directory if publication for that type of digital certificate is prescribed by the CP.

4.7.7 Notification of certificate issuance by the CA to relying parties

"No stipulation".

4.8 Certificate Modification

No special procedure is provided for the modification of certificates. All changes to digital certificates will be treated as a certificate re-key, and therefore performed as defined in section 4.7.

Therefore, the remaining subsections 4.8.1 to 4.8.7 from RFC 3647 are not included in the CP and should be marked "No stipulation".

4.9 Revocation and suspension of digital certificate

Certificate revocation is the action of rendering a certificate invalid prior to its expiry date. Revocation is published in a public register of revoked certificates (CRL – Certificate Revocation List).

4.9.1 Circumstances for certificate revocation

Digital certificate revocation may be due to the following:
- the private keys of the holder are suspected to have been or have been compromised or endangered in a way that affects reliability of usage
- a change in the data contained in the certificate
- a failure to comply with the requirements set by the CP
- the certificate holder has violated the requirements of appropriate use
- the certificate holder has terminated its working relationship with the BS
- a formal request for revocation has been received

4.9.2 Who can request certificate revocation

A certificate revocation request may be sent by the following:
- a digital certificate holder
- the BS department manager of the certificate holder or the BS department manager who initiated the contract with the organization of the certificate holder
- CA personnel upon discovering that:
    - the certificate holder has terminated its working relationship with the BS
    - circumstances that have had a major impact in on the validity of the digital certificate have changed
    - the information contained in the certificate is not correct
    - the CA will stop issuing digital certificates or is no longer authorized to issue digital certificates
    - the infrastructure or the private keys of the CA have been compromised or endangered in a way that affects reliability of usage

- the infrastructure or the private keys of the holder have been compromised or endangered in a way that affects reliability of usage

4.9.3 Procedure used for certificate revocation request

A digital certificate issued by the CA at the BS may be revoked according to the standard procedure or the extraordinary procedure.

The standard procedure is used during the CA's ordinary working hours (between 6.30 am and 5 pm on working days). A revocation request in the standard procedure may be sent to the CA as follows:
the certificate holder requests the revocation in person at the CA's RA;
-
the request to revoke the digital certificate is sent to the CA's email address (see Section 1.3.1) by the certificate holder or the responsible person at the BS department at which the holder is employed, or by the initiator of the BS's contractual relationship with the holder. The message with the request must be electronically signed with their own digital certificate issued by the CA at the BS. At the same time they must inform the CA by calling the telephone number for certificate revocations (see Section 1.3.1).

The extraordinary procedure is used outside of the CA's ordinary working hours (between 5 pm and 6.30 am on working days, and at weekends and on public holidays). In the extraordinary procedure the digital certificate holder may request revocation by calling the telephone number for certificate revocations (see Section 1.3.1). In this event the CA's RA suspends the digital certificate (according to the procedure set out in Section 4.9.15).

The grounds for revocation must be cited in the revocation request.

When the RA receives a request to revoke a digital certificate, it checks whether the request contains all the required data, validates the identity of the sender of the revocation request, and checks that the grounds for revocation accord with those cited in Section 4.9.1.If the request is rejected, the RA will notify the sender.

In addition to the aforementioned procedures for standard and extraordinary revocation, the personnel of the CA may revoke a holder's digital certificate when they learn that one of the grounds for revocation of a digital certificate cited in Section 4.9.1 has been met.

The personnel of the CA inform the holder of the digital certificate of the revocation of the digital certificate, the date of revocation and the grounds for revocation.

If key archiving is envisaged for this type of digital certificate, the CA will keep an archived copy of the key pair that corresponds to the revoked digital certificate. The archived copy of the key pair may be recovered as detailed in section 4.12.

4.9.4 Grace period available to holder to prepare the revocation request

Persons with the right to send a revocation request must prepare the revocation request as soon as they have identified one of the circumstances for certificate revocation.

4.9.5 The time within which the CA should process revocation requests

All valid revocation requests received by the CA are processed as quickly as possible, and in any case within one hour of the request being received.

4.9.6 Revocation checking requirements for relying parties

Before using digital certificates issued by the CA, all relying parties are responsible for checking the CRL published by the CA. Relying parties must check the validity of the CRL and download the most recent version of the CRL published on the CA website as defined in section 7.2. The address where the CRL is published is also contained in the "CRL distribution point" field of all digital certificates issued by the CA. The CRL is digitally signed by the CA private key used to sign the digital certificates issued.

4.9.7 The CRL issuance frequency

The validity period and issuance frequency of the CRLs are defined in Table 4 below.

Table 4: CRL validity period and issuance frequency

The CA server	CRL Validity period	CRL Issuance frequency
Banka Slovenije CA Root	1 year	Every year
Banka Slovenije CA Ent SUB (full register)	7 days	Every day
Banka Slovenije CA Ent SUB (changes)	1 day	Every day

The new CRL is published before the old one expires.

Whenever a digital certificate is revoked, the personnel at the RA manually initiate the publication of a new CRL.

4.9.8 Maximum latency between the generation of CRLs and their publication

The maximum time allowed between the generation of the CRL and its publication in the repository is one hour.

4.9.9 Online certificate revocation status checking

Online digital certificate status verification is available over the HTTP and OCSP protocols.

4.9.10 Online revocation checking requirements

When using digital certificates, relying parties must always verify if the certificate they rely on has been revoked.

4.9.11 Other forms of revocation alerts available

"No stipulation".

4.9.12 Special requirements for the revocation of compromised keys

"No stipulation".

4.9.13 Grounds for suspension of a digital certificate

Suspension of a digital certificate is a procedure that results in the digital certificate becoming inoperative before its expiration. Suspension is always temporary in nature, i.e. of limited duration. The suspension of a digital certificate prevents it from being used by the holder. For the duration of the suspension the digital certificate is listed on the CRL.

A digital certificate may be suspended in the following cases:
- suspected disclosure of the private key related to that digital certificate
- when the personnel of the CA receive a request to revoke a digital certificate, but cannot verify the authorisation of the person that submitted the request (e.g. revocation of a digital certificate according to the extraordinary procedure)

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

Suspension of a digital certificate may be requested by:
- the holder of the digital certificate
- the personnel of the CA in the event of the suspected disclosure of the private key related to that digital certificate

Suspension of a digital certificate may be cancelled by the CA's RA.

4.9.15 Procedure for suspension of a digital certificate

In the event of suspected disclosure or any other identified threat to private key related to a digital certificate, the holder of the digital certificate immediately sends a request to suspend the digital certificate to the CA's RA.

The revocation of a digital certificate according to the extraordinary procedure (as defined in Section 4.9.3) is also classed as a request to suspend the digital certificate. Because the extraordinary procedure for the revocation of a digital certificate does not allow for the identity of the sender of the request to be verified, the personnel of the CA's RA suspend the digital certificate in this case until they receive a request to revoke the digital certificate or a request to cancel the suspension of the digital certificate via the ordinary procedure.

When the CA's RA receives a request to suspend a digital certificate, it validates the identity of the sender of the request and checks that the grounds for suspension of the digital certificate accord with those cited in Section 4.9.13. If there are no grounds for refusing the request for suspension, the personnel of the CA's RA suspend the digital certificate and initiate the procedure for updating and publishing the CRL. If the request for suspension is refused, the CA's RA informs the sender of the request accordingly.

The personnel of the CA's RA inform the holder of the digital certificate of the suspension of the digital certificate, the date of suspension, and the grounds for suspension.

4.9.16 Duration of suspension of a digital certificate

The suspension of a digital certificate remains in effect unless the personnel of the CA cancel the suspension. The maximum time that may elapse between the suspension of a digital certificate and the cancellation of the suspension is one working day.

4.10 Certificate Status Services

4.10.1 Operational characteristics

The CRL is accessible at the addresses defined in sections 7.2 and 7.3. The address where the CRL is published is also contained in the "CRL distribution point" field of all digital certificates issued by the CA.

4.10.2 Service availability

The CA is committed to providing the CRL service 24 hours a day, 365 days of the year at a yearly availability rate of 99.5% (this basis excludes preventive maintenance).
This high level of availability is detailed in the CPS.

4.10.3 Additional features

"No stipulation".

4.11 Termination of the relationship between the holder and the CA

The relationship between the holder and the CA is established with the acceptance of the BS ID card.

Relationship is terminated due to the following:
- regular expiry of the certificate and no certificate re-key has been requested
- early certificate revocation without a re-key having been requested or the request was rejected

4.12 Key Escrow and Recovery

4.12.1 Key Archive and recovery policies

A key escrow service is not envisaged.

Private keys that can be used for digital signature or authentication are always generated inside the cryptographic token of the BS ID card. Therefore key archive and recovery is not provided for this type of key.

The CA archives copies of private keys that can be used for encryption. Archived copies are performed as defined in section 6.2.4.

4.12.1.1 Key recovery procedure

Only a certificate holder may request the recovery of the private key used for encryption.
The holder must be present at the RA premises during recovery. The key pair must be recovered on the BS ID card issued and personalized to the name of the certificate holder.

During recovery only secure protocols may be used between the key recovery service and the cryptographic module of the BS ID card.

This procedure is detailed in the CPS.

4.12.1.2 Key disclosure procedure

Only the Governor of the BS or law enforcement authorities may request the disclosure of private keys used for encryption.

At least one of the two Key Recovery Officers (KRO) and one representative of the RA must participate in the key disclosure process.

This procedure is detailed in the CPS.

4.12.2 Session key protection

When transferred, the session key must always be encrypted.

This procedure is detailed in the CPS.

5 Management, Operational and Physical controls

5.1 Physical security controls

Physical security controls ensure the physical security of the CA premises. These requirements are aligned with the requirements defined by the policies and standards for the physical security of the BS computer center premises. The controls established are detailed in the CPS and cover the following topics:

- site location and construction
- physical access
- power and air conditioning
- water exposure

- fire prevention and protection
- media storage
- waste disposal
- off-site backup

5.2 Procedural security controls

Procedural security controls ensure the adequate segregation of duties among CA stakeholders, so as to reduce the risk of accidental or deliberate misuse. The controls established are detailed in the CPS and cover the following topics:

- the CA organizational structure and allocation of roles
- the number of individuals required per task
- the identification and authentication requirements for each role
- roles requiring separation of duties

5.3 Personnel security controls

The personnel security controls established are detailed in the CPS and cover the following topics:

- qualifications, experience and authorization requirements
- background check procedures
- initial training requirements
- ongoing training requirements and frequency
- frequency and sequence for job rotation
- disciplinary measures for unauthorized actions
- requirements with respect to third party contracting
- documentation supplied to personnel

5.4 Audit logging procedures

Audit logging requirements ensure the authenticity and integrity of log files. The controls established are detailed in the CPS and cover the following topics:

- type of events to be recorded
- frequency of audit log processing
- audit log retention
- audit log protection
- audit log backup procedure
- audit log collection system
- providing notification that an event has been logged to the person who caused the event
- vulnerability assessment

5.5 Data Archival

5.5.1 Types of records that are archived

The CA stores the following data and documents:
- logs defined in section 5.4
- certificate application forms including the holder's statements of acceptance of the terms and conditions for the use of digital certificates issued by the CA in accordance with the CP
- certificate revocation requests
- digital certificates
- revisions of the CP and the CPS
- holder's encryption private keys

5.5.2 Archive retention period

Correspondence with the CA and contracts are stored for 20 years.
Certificates, the CRL and private keys are stored for a minimum of 20 years.

5.5.3 Archive protection

Access to archived data is protected by the same controls that are established in the CA computer center.

5.5.4 Requirements for time-stamping of records

"No stipulation".

5.5.5 Archive collection system

"No stipulation".

5.5.6 Procedures to obtain and verify archived data

The archives may be made available to the authorized persons of the CA detailed in the CPS.

5.6 Key Changeover

The CA may issue only digital certificates with an expiry date that does not exceed the expiry date of the CA's private key used to sign the certificates.

Procedures performed by the CA to extend the validity of its own private key and corresponding digital certificate are detailed in the CPS.

The CA plans the implementation of the procedures to extend the validity of its own certificates so as to pose no threat to the continuity of services that depend on the validity of each CA's digital certificates.

5.7 Compromise and Disaster Recovery

Recovery procedures in the event of security incidents or if the CA's private key is compromised are detailed in the CPS and cover the following topics:
- procedures for reporting and handling incidents and compromise events
- recovery procedures in the event that hardware, software or data become corrupted
- recovery procedures in the event that the private key of the CA component is compromised
- business continuity capabilities following an incident

5.8 CA or RA Termination

In the event of termination of its activities, the CA will carry out the following:
- notify all holders and publish information regarding the termination of its activities
- revoke all digital certificates signed by the CA that are still valid
- securely destroy its private keys, securely dispose of its equipment and keep records of progress. All activities are carried out according to the four-eyes principle;
- ensure continuity of the revocation service in accordance with the service availability requirements detailed in the CP for six (6) months after all digital certificates have been revoked
- transfer the CRL service to an external CA
- ensure the continuity of the archive function for five (5) years after termination

6 Technical Security controls

6.1 Key pair Generation an Installation

6.1.1 Key pair generation

6.1.1.1 The CA keys

The CA key pairs are generated following the formal procedure for the setup of the CA's infrastructure, detailed in the documents "ROOT CA G2 Key Generation Ceremony script in Banka Slovenije" and "ENT SUB CA G2 Key Generation Ceremony script in Banka Slovenije". Key pairs are generated in the cryptographic Hardware Security Modules (HSM) which are compliant with CC EAL4+ or a higher certification.

6.1.1.2 Holder keys

The procedure to generate holder key pairs depends on the type of digital certificate issued:

- for digital certificates that can be used for authentication and for digital certificates that can be used for digital signature, key pairs are generated on the cryptographic token of the BS ID card. The cryptographic token is compliant with the EAL 4+ or higher specification
- for digital certificates that can be used for encryption/decryption, the key pair is generated in the cryptographic Hardware Security Modules (HSM) compliant with FIPS 140-2 Level 3 or higher certification. As part of the key generation procedure a copy of the key pair is stored in the CA Key Archive service that uses a cryptographic module with the same requirements. Another copy of the key pair is safely transferred and stored inside the cryptographic token of the BS ID card. The cryptographic token is compliant with the EAL 4+ or a higher specification.

6.1.2 Private Key delivery to holder

For digital certificates that can be used for authentication and for digital certificates that can be used for digital signature, key pairs are generated and stored on the cryptographic token of the BS ID card. The holder accepts the private keys by accepting the BS ID card.

For digital certificates that can be used for encryption/decryption, standardized secure protocols are used during the key generation or key recovery procedure to transfer the key pair between the CA infrastructure components (e.g. HSM, ID Card Management System, Key Archive Service) and the cryptographic token of the BS ID card. Therefore no key delivery is required.

6.1.3 Holder's Public key delivery to the CA server

For digital certificates that can be used for encryption/decryption, a public key is generated by the CA server and so delivery to the CA server is not applicable.

For digital certificates that can be used for authentication and for digital certificates that can be used for digital signature, a public key is generated and stored on the cryptographic token of the BS ID card. Standardized secure protocols are used to transfer the public key between the BS ID card and the CA server.

6.1.4 The CA public key delivery to holders

The CA public key is accessible on the CA website at URL: http://ca.bsi.si/pki

Digital certificates are digitally signed and so the integrity of the published public key is guaranteed.

The authenticity of the published public key can be verified with the fingerprint published on the CA website (above) or over the telephone (section 1.3.1).

6.1.5 Key size

The CA uses a 4,096 bit RSA private keys.

Holders use a 2048 bit RSA key.

6.1.6 Key pair parameter generation

The parameters for generating RSA keys meet the PKCS#1 specifications. All key pair parameters for the CA key pairs and holder key pairs are generated in the HSM and in the cryptographic module of the BS ID card respectively.

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

The keyUsage field defines the accepted key usage for each type of digital certificate and is contained in all digital certificates issued by the CA. Digital certificate accepted key usage is detailed in Table 5.

Table 5: "KeyUsage" field

Type of digital certificate	Key usage field
Encryption	Encryption: 1
Signature	Non repudiation: 1
Authentication	Digital Signature:1

Additional constraints may be defined in the Extended Key Usage field.

Table 6: "Extended key usage" field

Type of digital certificate	Extended Key usage field
Encryption	Any Purpose (2.5.29.37.0) Secure Email (1.3.6.1.5.5.7.3.4) Encrypting File System (1.3.6.1.4.1.311.10.3.4)
Signature	Document Signing (1.3.6.1.4.1.311.10.3.12) Secure Email (1.3.6.1.5.5.7.3.4) Any Purpose (2.5.29.37.0)
Authentication	Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2)

The CA private key may be used for signing:
- The holder's digital certificates
- CRLs

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

In order to generate and store its own private keys, the CA uses HSM that is compliant with the FIPS 140-2 level 3 specification.

Therefore, the installation and configuration of CA software includes the following tasks:
- start of the HSM
- generation of the HSM Administrator Card Set (ACS) and Operator Card Sets (OCS)
- generation of the CA private and public keys

CA personnel and digital certificate holders use cryptographic tokens of the BS ID card which is compliant with the CC EAL4+ or a higher specification.

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

The CA private keys are under multi-person control, which is detailed in the CPS.

6.2.3 Private Key Escrow

"No stipulation".

6.2.4 Private Key Backup

The CA private key backup

The private keys of the CA are backed up. Backup copies are encrypted with the private key stored on the HSM operator card set.

Holder's private key backup

The holder's private keys that can be used for encryption are backed up. Backup copies are encrypted with the private key stored on the HSM operator card set.

6.2.5 Private Key Archive

The CA archives backup copies of the holder's encryption private key and has procedures in place to recover the private key on the BS ID card of the holder. This procedure is detailed in section 4.12.1.

6.2.6 Private Key transfer to cryptographic module

The CA private keys are generated and stored in the HSM; therefore, transmission of this key to the HSM is not applicable.

The holder's private keys that can be used for authentication and the private key that can be used for digital signature are generated and stored in the cryptographic module of the BS ID card; therefore, the transmission of these keys to the cryptographic module of the Bank of Slovenia ID card is not applicable.

The holder's private key that can be used for encryption is generated and stored on the HSM and transferred to the cryptographic module of the BS ID card during the card personalization process. Secure standardized protocols are used for transmission.

6.2.7 Private Key storage in a Cryptographic Module

The CA's private keys may be activated only on the HSM.

The holder's private keys are stored in the cryptographic module of the BS ID card.

6.2.8 Private Key activation method

The CA private keys used for signature are activated during the CA software start-up. To activate the private keys, OCS cards with the corresponding PINs are required.

The holder's private keys are protected with a PIN which has to be entered in order to activate the private key.

6.2.9 Private Key deactivation method

The CA private keys are deactivated by the shutdown of CA software.
The holder's private keys are deactivated by removing the card from the reader. Some applications also provide deactivation following a time-out period.

6.2.10 Private Key destruction method

The CA private keys are destroyed at the end of the private key's lifespan, following the controlled procedure.

All holders' private keys are destroyed at the end of subscription or in the event of physical damage to the cryptographic module of the BS ID card.

A private key that can be used for authentication and a private key that can be used for digital signatures are deleted from the BS ID card during the certificate re-key procedure.

6.2.11 Cryptographic Module Capabilities

Detailed in section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archiving

The CA public key and holder's public keys are archived as detailed in section 5.5.

6.3.2 Operational period of issued digital certificates

The operational period for digital certificates issued by the CA is aligned with the operational period for the corresponding private key.

The validity of the CA public key used for the verification of digitally signed data is 30 years.
The validity of the CA private key used for a digital signature is 30 years.
The validity of the subordinate CA public key used for the verification of digitally signed data is 15 years.

The validity of the subordinate CA private key used for a digital signature is 15 years.

The validity of a holder's private keys used for authentication is 5 years.
The validity of a holder's public keys used for the verification of digitally signed data is 5 years.
The validity of a holder's private keys used for digital signature is 5 years.
The validity of a holder's public keys used for encryption is 5 years.
The validity of a holder's private keys used for decryption is unlimited.

6.4 Activation Data

6.4.1 Generation and installation of activation data

The HSM activation data is generated during the HSM initial installation by the CA's authorized personnel who must know the activation data in order to perform the tasks for which they are responsible. The activation data are the ACS and OCS cards' PIN numbers.

The activation data of the cryptographic module on the BS ID card is generated during the initial installation and personalization of the card. The activation data is securely delivered to the holder. This procedure is detailed in the CPS. The activation data is the PIN needed to activate the private keys stored in the cryptographic module of the card. Holders are obliged to change the PIN after first use of the card.

6.4.2 Activation Data protection

The activation data is safely stored in order to protect its confidentiality and integrity until they reach the final recipient, who is then responsible for ensuring the confidentiality, integrity and availability of the activation data. This procedure is detailed in the CPS.

6.4.3 Other aspects of activation data

"No stipulation".

6.5 Computer Security Controls

6.5.1 Specific security technical requirements

The controls established are detailed in the CPS and cover the following topics:
- the CA applications access control and segregation of access rights
- strong authentication with the use of cryptographic modules for CA personnel
- end-to-end session encryption
- CA database access control
- securing archive and log files
- audit functions
- data backups

6.5.2 Compure system security rating

All the hardware and software components used by the CA are hardened in accordance with vendor recommendations and best practices.

The requirements and procedures are detailed in the CPS.

6.6 Lifecycle security controls

6.6.1 System development controls

The BS shall ensure that all hardware and software components used by the CA are developed and implemented in compliance with the BS Information System Security Policies.

6.6.2 Security management controls

The CA must establish incident, problem and change management procedures. All changes must be logged.

The CA must establish procedures for monitoring software integrity.

6.7 Network security controls

The CA must ensure that network access is limited to connections needed to use and manage the CA infrastructure.

The controls established are detailed in the CPS.

6.8 Time-stamping

All systems used by the CA are synchronized with the public NTP servers.

7 Certificate and CRL profiles

7.1 Certificate profiles

7.1.1 Version number

The CA issues digital certificates using the X.509 Version 3 standard in accordance with PKIX recommendations.

All digital certificates contain the following general fields:

Signature
Issuer
Validity
Subject
SubjectPublicKeyInformation
Version
SerialNumber

7.1.2 Certificate extensions

Certificate extensions are used for the additional attributes of X.509 v3 digital certificates. Standard extensions are defined in accordance with RFC5280 and so the CA is allowed to define and add its own extensions.

7.1.2.1 Standard Extensions

The CA uses the following standard extensions:

Attribute name	**Description**
authorityKeyIdentifier	Thumbprint of the CA's public key used to sign the digital certificates issued (added by the CA server)
subjectKeyIdentifier	Thumbprint of the holder's private key (added by the CA server)
KeyUsage*	As detailed in section 6.1.7
extKeyUsage	As detailed in section 6.1.7
privateKeyUsagePeriod	As detailed in section 6.3.2
certificatePolicies	OID of the CPS, OID of digital certificate type and URL where the CP is published.
cRLDistributionPoints	URL where the CRL is published.
Authority Information Access	URLs where the CA digital certificate, and

Attribute name	Description
	OCSP status checking can be accessed.
subjectAlternativeName	Holder's e-mail address.
basicConstraints	Added by the CA server
ETSI TS 101 862 Qualified Certificates	Qualified Digital Certificate Statement
EU Qualified Certificate Policy	CP
QCStatements	The extension is used in qualified certificates in accordance with ETSI EN 319 412-5.

***Critical fields:** End user applications must process critical fields in accordance with PKIX recommendations.

7.1.3 Algorithm Object Identifiers (OID)

All algorithms are used in accordance with valid standards and recommendations.

7.1.4 Name formats

Digital certificates issued by the CA contain the issuer's and holder's distinguished name in the fields "issuer name" and "subject name", as detailed in section 3.1.1

7.1.5 Name constraints

As detailed in section 3.1.1.

7.1.6 Certificate Policy Object Identifiers (OID)

Digital certificates issued by the CA contain one or more issuance policy OIDs. The CA use the field *"certificatePolicies"* to mark this type of certificate. The CP identifiers are detailed in section 1.2.

7.1.7 Use of the "Policy Constraints" extension

"No stipulation".

7.1.8 Syntax and semantics of the "Policy qualifiers"

The CA use the field *"PKIX policy qualifier"* for the URL where the CP and CPS are published.

7.1.9 Processing semantics of the critical "Certificate Policy" extension

Applications must process extensions in accordance with the RFC5280 recommendations for critical extensions.

7.1.10 Unique Electronic Identification Number

In accordance with Article 24 of the Electronic Identification and Trust Services Act (Official Gazette of the Republic of Slovenia, Nos. 121/21 and 189/21 – ZDU-1M), and Article 52 of the Regulation on the Determination of Electronic Identification Means and the Use of the Central Service for Online Login and Electronic Signature (Official Gazette of the Republic of Slovenia, No. 29/22), the Unique Electronic Identification Number of the holder is recorded in the qualified certificate for electronic signature, electronic seal, or website authentication as a private extension of the qualified certificate.

This is recorded as a separate extension field, written in ASN.1 notation:
SEQUENCE :
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.1' <OID of the extension for the value of the Unique Electronic Identification Number of a natural person>
OCTET_STRING :
IA5String : 'xxxxxxxxxxxx' <value>
SEQUENCE :
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.2' < OID of the extension for the value of the Unique Electronic Identification Number of the business entity>
OCTET_STRING :
IA5String : 'xxxxxxxxxxxx' <value>

7.2 CRL profile

The valid CRL is the most recent version published at the address defined in Table 7.

Table 7: CRL publication address

The CA server	HTTP address	OCSP address
Banka Slovenije Root CA G2	http://ca.bsi.si/pki/crls/Banka Slovenije Root CA G2.crl	
Banka Slovenije Ent Sub CA G2	http://ca.bsi.si/pki/crls/Banka Slovenije Ent Sub CA G2.crl	http://ocsp.bsi.si/ocsp

7.2.1 Version number

CRL is X.509 Version 2 and is published in accordance with PKIX Part 1 recommendations.
CRL contains the following fields:

Version	V2
Signature	The CA signature
Issuer	Distinguished name
thisUpdate	Time of CRL issue
nextUpdate	Time of next CRL issue

revokedCertificate	Serial numbers of revoked certificates

7.2.2 CRL and extensions

In accordance with PKIX Part 1 recommendations, the CA use the following X.509 Version 2 CRL and ARL-extensions:

cRLNumber	Added by the CA server
reasonCode	Reason is not published
holdInstructionCode	"No stipulation"
invalidityDate	Added by the CA server if data is contained in the request
issuingDistributionPoint	Added by the CA server
certificateIssuer	"No stipulation".
deltaCRLIndicator	"No stipulation".

7.3 OCSP profile

Digital certificate online status checking is available at URL: http://ocsp.bsi.si/ocsp.

8 Compliance Audit and Other Assessment

Compliance audits and assessments are performed in accordance with Bank of Slovenia requirements.

Internal and external audits and assessments are performed.

8.1 Frequency of compliance audit and other assessment

Internal audits are performed at least once per year.

External audits are performed in accordance with business needs.

8.2 Identity and qualifications of auditors and assessors

Audits and assessments may be performed by the following:
- information security auditors at the BS;
- The BS Audit department
- Other external auditors, assessors or other competent external entities

The CA shall give its authority for auditing or assessing a component to an audit team with expertise in information system security and the component's area of activity.

8.3 The relationship between the assessor and the entity being assessed

CA personnel may not perform audits and assessments of tasks from within their own scope of responsibility.

The auditor or assessor must be duly authorized to perform the audit or assessment in question.

External auditors and assessors are selected through public tenders or by virtue of their duties. Before performing an inspection, the BS and external entity must sign a contract which ensures non-disclosure and details the scope of inspection.

8.4 Scope of audits and assessments

Audits and assessments may cover the following topics:
- CA infrastructure
- CA processes and procedures
- compliance with the CP and CPS
- compliance with legislation

8.5 Actions taken as a result of deficiencies

After each inspection the CA prepares a plan of corrective actions to eliminate the deficiencies identified.

8.6 Notification of the results

The CA shall notify the BS IT department management, the Chief Information Security Officer and Risk Management Board of the results of the audits and assessments.

9 Other Business and Legal Matters

9.1 Fees

"No stipulation".

Therefore, the remaining subsections 9.1.1 to 9.1.4 from RFC 3647 are not included in the CP and should be marked "no stipulation".

9.2 Financial Responsibility

9.2.1 Liability insurance

For the risks inherent in the use of digital certificates that it issues, the CA holds general liability insurance of a scope defined by contract.
In addition Banka Slovenije maintains sufficient reserves to cover any cost arising on this part.

9.2.2 Other Assets

"No stipulation".

9.2.3 Insurance or warranty coverage for holders

"No stipulation".

9.3 Confidentiality of Business Information

9.3.1 The scope of Confidential Information

The following data is treated as confidential:
- the CA's and holder's private keys
- the CA's and holder's private key activation data
- audit logs
- certificate revocation requests
- digital certificate applications and corresponding data
- the holder's personal data

9.3.2 Information not within the scope of confidential information

Information contained in a digital certificate, certificate revocation list (CRL), or other information published on the issuer’s website is not considered confidential.

9.3.3 Responsibility to protect confidential information

The CA will protect confidential information in accordance with the legislation.

9.4 Privacy of Personal Information

9.4.1 Personal information protection plan

The personal information protection plan is defined in section 9.3 and from 9.4.2 to 9.4.7.

9.4.2 Protected personal information

The CA protects all personal data received or generated by performing its services except for the personal data defined in section 9.4.3.

9.4.3 Information not deemed personal

All data cited in the holder's digital certificate and in the CRL that is publicly accessible is deemed unprotected personal data.

9.4.4 Responsibility to protect personal information

The CA will protect personal information in accordance with the legislation and internal regulations governing personal data protection.

Before the issuance of a digital certificate within the framework of the CP applicable at the time (a published bylaw of the CA), the holder of the digital certificate is informed which personal data will be entered in the certificate and which other personal data is processed in connection with the issuance of the certificate.

By approving the application for a digital certificate, the holder of the digital certificate confirms their awareness of the rules with regard to personal data processing as proceeds from this CP or the CP applicable at the time.

9.4.5 Notice and consent to use personal information

The CA may use personal information only for the purposes authorized by the holder and on the basis of the written consent of the holder.

The legal basis for data processing is the employment contract or the contract for services, where the personal data is processed in connection with the performance of the contract.

9.4.6 Disclosure of personal information

The CA may disclose personal data only with the written consent of holder or at the request of the competent Court or Administrative Body.

9.4.7 Other circumstances to disclose personal information

"No stipulation".

9.5 Intellectual Property Rights

The BS is the owner of all rights related to the CA private keys, holder private keys, the CP, the CPS and all the documentation related to the issue of digital certificates.

9.6 Representations and Warranties

9.6.1 Obligations of the CA

The CA shall have the following obligations:
- to carry out their operations in accordance with this CP and applicable legislation
- to protect private keys
- to issue digital certificates in accordance with the CP
- to verify the validity of received applications to issue digital certificates in accordance with X.509 v3
- to issue and publish digital certificates as defined in the CP and the CPS
- to process revocation requests in a timely manner
- to publish the CRL in a timely manner as defined in the CP and the CPS
- to ensure the availability of the CRL in accordance with the CP and the CPS
- in the event of ceasing its activities, to notify the holders in in a timely manner
- to keep a record of all related information for each digital certificate issued for at least as long as defined in section 5.5.2.
- to ensure consistency of the data used for the creation and verification of digital signatures

9.6.2 Obligations of the RA

The RA shall have the following obligations:
- to verify the identity of applicants in accordance with the CP and the CPS
- to inform the applicant of the terms and conditions for the use of digital certificates issued by the CA
- to process applications for digital certificates in accordance with the CP and the CPS
- to submit complete, accurate valid and duly authorized certificate applications to the CA
- to store in a safe and prompt manner all the documentation provided in the process of issue, suspension or revocation of digital certificates
- to carry out other duties prescribed by the CP and the CPS

9.6.3 Obligations of certificate holders

The holders shall have the following obligations:
- to provide full, accurate and truthful information in certificate applications
- to inform the CA of any modification to data contained in digital certificates
- to understand and accept the terms and conditions for the use of digital certificates issued by the CA
- to restrict the use of digital certificates to that permitted under the CP
- to protect the accepted ID card of the BS from damage, loss, disclosure, modification and unauthorized use
- to generate a hard-to-guess PIN code used to protect private keys and to ensure confidentiality of the PIN code
- to immediately request revocation upon becoming aware of any compromise of the private key contained in the certificate
- to not monitor, manipulate of carry out any reverse engineering of the technical implementation of the certificate services
- to not transfer or delegate their obligations related to the use of digital certificates to third parties
- to regularly monitor notifications published on the CA website

9.6.4 Obligations of relying parties

Relying parties who accept and rely on the certificates issued by the CA shall have the following obligations:
- to limit reliability on the certificates to the uses prescribed by the CP
- upon receiving the digitally signed data, to verify that the digital certificates used for signature have not expired or been suspended or revoked
- to correctly verify the validity of the digital signature
- to verify the validity and suspension or revocation status of digital certificates on which they rely
- to be aware of the guarantees and responsibilities derived from acceptance of the certificates on which they rely
- to notify the CA of any circumstances which could compromise the private keys of the holders and should be considered cause for revocation

9.7 Disclaimers of Warranties

The CA shall not be held liable for any damage, loss, compensation or other claims occurring due to the following:
- the digital certificate that was issued because of inaccurate or invalid data provided by the holder
- expiry, suspension or revocation of the digital certificate
- use of digital certificate outside the scope permitted by the CP
- the inappropriate use or abuse of the digital certificate or the CRL
- the actions of the certificate holder or relying party that do not comply with the CP
- the abuse or breach of the information system of the holder
- the holder's permission given to third parties for the use of his or her digital certificates
- the failure or malfunction of holders or the relying party's computer system
- the failure or malfunction of infrastructure not managed by the CA
- force majeure

9.8 Limitations of Liability

The CA assumes no other commitment, gives no other guarantee, and shall accept no other liability regarding certificate holders and relying parties except those stipulated by the CP.

9.9 Indemnities

The CA assumes no financial responsibility for the use of digital certificates that are not compliant with the CP and applicable legislation.

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

Validity of the CP is terminated for the following reasons:
- a new version of the CP is put into force
- a change to the CA private key used to sign issued certificates
- a cessation of CA services

9.10.3 Consequences of the termination

If the CP is substituted with a new version, holders can use the existing certificates until they expire, in accordance with the terms and conditions stipulated by the version of the CP under which the certificates were issued. If the circumstances change the CA will notify the holders.

9.11 Individual notices and communications with participants

All notifications for holders and relying parties are published on the CA website at the URL defined in section 2.1.

9.12 Amendments

9.12.1 Amendment procedures

All typographic, editorial or content modifications with a non-significant impact on CA operations may be performed as an amendment to the existing CP.

All other changes must be performed as a CP with a new OID.

All amendments and changes to the CP are adopted in accordance with the same procedure as the CP.

9.12.2 Notification period and mechanism

Amendments shall be published on the CA website 3 days prior to the beginning of validity.

New versions of the CP shall be published on the CA website on the day of coming into force.

The CA shall notify all holders, relying parties and recognized external CAs of all amendments and new versions of the CP on its website.

9.12.3 Circumstances in which the OID must be changed

The CA decides when changes or amendments require a new OID for the CP following the criteria defined in section 9.12.1.

9.13 Dispute resolution procedures

Clients will strive to settle their disputes by agreement; if this proves impossible, the Court in Ljubljana shall be competent to settle them.

9.14 Valid legislation

The laws and regulations valid in The Republic of Slovenia shall apply, namely:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),
- The Electronic Identification and Trust Services Act,
- The Personal Data Protection Act,
- The Protection of Documentary and Archival Materials and Archives Act,
- The Decree on the Determination of Electronic Identification Means and the Use of the Central Service for Online Login and Electronic Signature,
- ETSI recommendations in the field of qualified certificates and trust services,
- RFC recommendations in the field of X.509 certificates,
- and other applicable regulations and recommendations.

9.15 Compliance with Applicable Law

The CA shall provide internal and external audits to ensure compliance with the applicable legislation.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement clause

All the relying parties accept the content of the latest CP.

9.16.2 Transfer of operations

The holder of a digital certificate may in no case transfer the rights and obligations in the use of digital certificates to a third party in part or in full.

9.16.3 Severability clause

If owing to changes in legislation or circumstances becomes part of the policy void the remaining parts shall remain in force until the publication of policy change.

9.16.4 Receivables

"No stipulation".

9.16.5 Force majeure

Force majeure describes an event that may arise after the relationship between the CA and the holder was established and is beyond the reasonable control of the parties (such as war, fire, earthquake, etc.).

If the force majeure event prevents the enforcement of the obligations under this document, the deadlines for completion shall be extended accordingly.

9.17 Other stipulations

The CP has been structured in accordance with the guidelines of the reference document RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*".

The “RULES OF THE CERTIFICATION AUTHORITY AT THE BANK OF SLOVENIA” enters into force on 18 April 2025. On this date the Certificate Policy version 3 shall cease to be in effect.

In Ljubljana, 9.4.2025