Name	**Certification Policy – ČSOB EDSS CA**
Type	Public document
Version	**1.0**
Issue date	**13.6.2022**
ID	**Certification Policy – ČSOB EDSS CA**
Description	This document specifies the applicability of a certificates issued by ČSOB EDSS CA for a particular usage, it defines the conditions on the certificates lifecycle, as well as it imposes the requirements on the operation of ČSOB EDSS CA.
Owner	IT Security
Classification level	Public
Environments	Production
Company	ČSOB, a.s.

Changes:

Issue date	Version	Change compared to the previous version	Changed (name)
26.4.2022	0.1	Initial draft, internal information included	Josef Kučera
9.6.2022	0.2	Updates 5.1, 5.2, removed internal information	Josef Kučera
13.6.2022	1.0	Final revision	Jiří Vábek

List of Content

1. INTRODUCTION

1.1 Overview

This document specifies the procedural and operational requirements that ČSOB requires to be adhered by the PKI Participants, when issuing and managing the certificates issued by ČSOB EDSS CA.

The certificates issued by ČSOB EDSS CA according to this policy, are issued using EDSS product developed by supplier.

This CP is only one of the documents that governs the ČSOB EDSS CA. Besides the regulatory documents, the internal ČSOB policies are applied.

To preserve the outline specified by RFC 3647, section headings that are not relevant have the statement "Not applicable" or "No stipulation."

1.2 Document Name and Identification

Name and identification of the document: Certification Policy – ČSOB EDSS CA, version 1.0.

OIDs are not used for the purpose of ČSOB EDSS CA and related objects.

1.3 PKI Participants

1.3.1 Certification authorities

This policy govern the CA called “ČSOB EDSS CA”. It is the subordinate issuing CA, issued by the offline root CA – “ČSOB EDSS Root CA”.

1.3.2 Registration authorities

The role of Registration authority is held by Sefira application EDSS, which is responsible for identification and authentication of certificate subject/client.

1.3.3 Subscribers

The Subscriber of the ČSOB EDSS CA are the clients, which are in some business relationship with ČSOB and which are required by ČSOB to sign documents provided by ČSOB via the certificates issued by ČSOB EDSS CA.

1.3.4 Relying parties

Relying parties are entities that rely on Certificates issued in accordance with this CP in their activities.

1.3.5 Other participants

Other participating entities are law enforcement authorities, or supervisory authorities, and others to whom this applies to trust-building services.

1.4 Certificate usage

1.4.1 Permitted certificate usage

The certificates issued by ČSOB EDSS CA are used for signing documents of the Subscribers.

1.4.2 Prohibited certificate uses

Certificates issued according to this CP, shall not be used for any other purpose than described in 1.4.1. A Certificate only establishes that the information in the Certificate was verified as reasonably correct when the Certificate issued, and it does not give any other guarantee.

1.5 Policy Administration

1.5.1 Organization administering the document

This CP is administered by ČSOB.

1.5.2 Contact person

The contact person for this CP is the person positioned in the role of the application manager of ČSOB EDSS application.

1.5.3 Person determining CPS suitability for the policy

No stipulation.

1.5.4 CPS approval procedures

No stipulation.

1.6 Definitions and Acronyms

CA	Certification Authority. If not specified differently, it stands specifically for ČSOB EDSS CA.
Certificate	An electronic document that uses a digital signature to bind a Public Key and an identity.
CP	Certification policy
CRL	Certificate Revocation List
ČSOB	Československá obchodní banka, a.s.
ČSOB PKI	Internal ČSOB Public Key Infrastructure
HSM	Hardware Security Module
Private Key	The key that is kept secret and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key that may be publicly disclosed and that is used to verify digital signatures created with the corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the corresponding Private Key.
RA	Registration Authority
SDLC	Secure Development Life-Cycle

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ČSOB store the information as certificates, policies and such according to internal regulations and rules for handling and classification of information.

2.2 Publication of certification information

ČSOB EDSS CA makes the following information publicly available on ČSOB public websites: all trusted CA certificates, root CA certificates and CPs.

2.3 Time or frequency of publication

ČSOB EDSS CA publish the CA certificates and CPs as soon as possible after they are issued or changed.

2.4 Access controls on repositories

All public information are published without limitation.

The internal and confidential information are handled in accordance with internal ČSOB rules for handling and classification of information, which are in compliance to regulatory requirements.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

All types of names are issued in accordance with valid technical standards.

3.1.2 Need for names to be meaningful

The names in some fields have a specific meaning that is described for the certificate profile (chapter 7.1.4.).

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of names

Serial number uniqueness is required in each Certificate issued by CA.

3.1.6 Recognition, authentication, and role of trademarks

Subscribers may not request Certificates with any content that violates the intellectual property rights of another entity. This CP does not require CA to verify a right of the Subscriber to use a trademark.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

Not applicable

3.2.2 Authentication of organization identity

Not applicable

3.2.3 Authentication of individual identity

Every individual acting with ČSOB must be authenticated respecting the principles set by the Czech and European law, international agreements such as AML and ČSOB and KBC group methodologies and guidelines. In the matter of certificate subscription, all dealings must be held in person with all participants proving their identity with an appropriate identification document, until means of trusted communication is set up (this may be but is not limited to encrypted e-mail communication).

The identification of the client's identity is performed by ČSOB systems, which require the issuance of a certificate for the given client.

3.2.4 Non-verified subscriber information

Not applicable.

3.2.5 Validation of authority

See 3.2.3.

3.2.6 Criteria for interoperation

Not applicable.

3.3 I&A for Re-key Requests

3.3.1 Identification and authentication for routine re-key

Not applicable.

3.3.2 Identification and authentication for re-key after revocation

Not applicable.

3.4 I&A for Revocation Requests

Not applicable.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

The CA can be contacted by internal ČSOB application (backend application component designed for this purpose) , that have permission for this request.

4.1.2 Enrolment process and responsibilities

All key operations within a given session for a given user are performed on the CA side.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

Described in chapter 3.2.2 and 3.2.3 for initial identification and authentication.

4.2.2 Approval or rejection of certificate applications

No stipulation.

4.2.3 Time to process certificate applications

CA generate the Certificate for the Subscriber immediately.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

No stipulation.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Not applicable

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation

4.4.2 Publication of the certificate by the CA

Not applicable.

4.4.3 Notification of certificate issuance by the CA to other entities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

The private key is operated in a secure ČSOB environment, which is governed by ČSOB's internal policies. This key will be permanently deleted when all document signing operations are completed. For certificate usage, see 1.4.

4.5.2 Relying party public key and certificate usage

Not applicable, see 1.3.4.

4.6 Certificate Renewal

The CA generates short-term keys and certificates (maximum 30 minutes) for signing documents, so there is no need for certificate renewal.

4.6.1 Circumstance for certificate renewal

Not applicable, see 4.6.

4.6.2 Who may request renewal

Not applicable, see 4.6.

4.6.3 Processing certificate renewal requests

Not applicable, see 4.6.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable, see 4.6.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable, see 4.6.

4.6.6 Publication of the renewal certificate by the CA

Not applicable, see 4.6.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable, see 4.6.

4.7 Certificate Re-key

The CA generates short-term keys and certificates (maximum 30 minutes) for signing documents, so there is no need for re-key.

4.7.1 Circumstance for certificate re-key

Not applicable, see 4.7.

4.7.2 Who may request certification of a new public key

Not applicable, see 4.7.

4.7.3 Processing certificate re-keying requests

Not applicable, see 4.7.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable, see 4.7.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable, see 4.7.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable, see 4.7.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable, see 4.7.

4.8 Certificate Modification

The CA generates short-term keys and certificates (maximum 30 minutes) for signing documents, so there is no need for certificate modification.

4.8.1 Circumstance for certificate modification

Not applicable, see 4.8.

4.8.2 Who may request certificate modification

Not applicable, see 4.8.

4.8.3 Processing certificate modification requests

Not applicable, see 4.8.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable, see 4.8.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable, see 4.8.

4.8.6 Publication of the modified certificate by the CA

Not applicable, see 4.8.

4.8.7 Notification of certificate issuance by the CA to other

Not applicable, see 4.8.

4.9 Certificate Revocation and Suspension

The CA generates short-term keys and certificates (maximum 30 minutes) for signing documents, so there is no need for revocation and suspension.

4.9.1 Circumstances for revocation

Not applicable, see 4.9.

4.9.2 Who can request revocation

Not applicable, see 4.9.

4.9.3 Procedure for revocation request

Not applicable, see 4.9.

4.9.4 Revocation request grace period

Not applicable, see 4.9..

4.9.5 Time within which CA must process the revocation request

Not applicable, see 4.9.

4.9.6 Revocation checking requirement for relying parties

Not applicable, see 4.9.

4.9.7 CRL issuance frequency

Not applicable, see 4.9.

4.9.8 Maximum latency for CRLs

Not applicable, see 4.9.

4.9.9 On-line revocation/status checking availability

Not applicable, see 4.9.

4.9.10 On-line revocation checking requirements

Not applicable, see 4.9.

4.9.11 Other forms of revocation advertisements available

Not applicable, see 4.9.

4.9.12 Special requirements related to key compromise

Not applicable, see 4.9.

4.9.13 Circumstances for suspension

Not applicable, see 4.9.

4.9.14 Who can request suspension

Not applicable, see 4.9.

4.9.15 Procedure for suspension request

Not applicable, see 4.9.

4.9.16 Limits on suspension period

Not applicable, see 4.9.

4.10 Certificate Status Services

There are no certificate status services.

4.10.1 Operational characteristics

Not applicable, see 4.10

4.10.2 Service availability

Not applicable, see 4.10.

4.10.3 Optional features

Not applicable, see 4.10.

4.11 End of Subscription

The CA generates short time certificates – 30 minutes expiration.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Security Controls

The components of the PKI infrastructure are located either in the ČSOB datacentres or in especially protected locations, according to the sensitivity of the component.

The physical security of the ČSOB locations and datacentres is managed according internal rules and described within internal documents, which are subject to relevant banking regulations and regular auditing, both internal and external. The detailed information is classified as internal / confidential.

5.1.1 Site location and construction

No stipulation, see 5.1.

5.1.2 Physical access

No stipulation, see 5.1.

5.1.3 Power and air conditioning

No stipulation, see 5.1.

5.1.4 Water exposures

No stipulation, see 5.1.

5.1.5 Fire prevention and protection

No stipulation, see 5.1.

5.1.6 Media storage

No stipulation, see 5.1.

5.1.7 Waste disposal

No stipulation, see 5.1.

5.1.8 Off-site backup

No stipulation, see 5.1.

5.2 Procedural Controls

Several roles are created for CA administration within ČSOB's internal processes. These are:

- EDSS configurator - CA configuration

- EDSS Application Manager - performs CA log analysis

- HSM administrator - configuration and analysis of HSM logs.

All CA configuration and management procedures are described in ČSOB's internal guidelines.

5.2.1 Trusted roles

No stipulation, see 5.2.

5.2.2 Number of persons required per task

No stipulation, see 5.2.

5.2.3 Identification and authentication for each role

No stipulation, see 5.2.

5.2.4 Roles requiring separation of duties

No stipulation, see 5.2.

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

Each role participating the operation of CA is required to be qualified according to the internal competence matrix for the positions.

5.3.2 Background check procedures

There are standard background checks applied for newly hired personnel according to the internal HR rules in ČSOB. There are no additional requirements applied for CA related roles.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

The contractor requirements are applied according to the internal ČSOB rules, as well as in accordance to regulatory requirements.

5.3.8 Documentation supplied to personnel

The CA personnel is provided with the internal ČSOB regulations, as well as the necessary documentation for their position to operate the PKI.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

All security relevant events are logged and are subject to security monitoring by SIEM, most importantly the audit logs concerning the events of:

- Private Key generation and manipulation
- Certificate requests – requesting and issuing
- Changes to the audit parameters
- Authentication attempts
- Changes to roles and authorization
- EDSS management

5.4.2 Frequency of processing log

The security monitoring of specified events is done by SIEM, reviewed on 24x7 basis.

For the key components of EDSS, there is define log rotation period for the critical logs.

5.4.3 Retention period for audit log

The retention of audit logs vary according to its type and included data and is governed by the internal rules of ČSOB for logging and auditing.

5.4.4 Protection of audit log

The critical audit logs are send to SIEM, where are protected from unauthorized access and reviewed by dedicated operators.

5.4.5 Audit log backup procedures

The audit log is backed up by the means of internal SIEM.

5.4.6 Audit collection system (internal vs. external)

The internal system is used for log collection.

5.4.7 Notification to event-causing subject

The event-causing subject are not notified about the log recording.

5.4.8 Vulnerability assessments

The EDSS infrastructure is regularly scanned for vulnerabilities by the common ČSOB tool for vulnerability assessment and the vulnerabilities are managed, according to the internal ČSOB rules.

5.5 Records Archival

5.5.1 Types of records archived

The electronic records connected with the CA that are archived are most importantly:

- CA Certificates and related defined data
- CP / CPS documentation, contractual documentation
- CA component documentation, operational documentation, procedural documentation

5.5.2 Retention period for archive

The retention period for archived information is individual, according to internal ČSOB rules, law regulations and business needs for each type of information.

5.5.3 Protection of archive

The archived information are protected by standard physical and logical security means, defined by the internal ČSOB standards.

5.5.4 Archive backup procedures

Not applicable.

5.5.5 Requirements for time-stamping of records

Not applicable.

5.5.6 Archive collection system (internal or external)

CA collects archive information internally.

5.5.7 Procedures to obtain and verify archive information

The information is kept either in online archive, otherwise the internal ČSOB procedures are followed.

5.6 Key Changeover

The CA periodically changes its Private Keys in a timely manner to prevent downtime in the operation. After key changeover, the CA signs Certificates using only the new key. The CA still protect its old Private Keys and the old Certificate is available to verify signatures until all of the Certificates signed with the old Private Key have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

In case of the incident, there are internal rules and processes, how to handle the various types of incidents, which are followed for CA operation as well.

The specific recovery procedures or the solutions for known issues are described in the internal operational documentation of CA and available to CA Administrator.

5.7.2 Computing resources, software, and/or data are corrupted

No stipulation, see 5.7.1

5.7.3 Entity private key compromise procedures

In case there is a justified suspicion that the CA private key is compromised, the CA Administrators should take the following actions:

- Assess the risk of a compromise and determine the degree and scope of the potential impact of a breach of the security of Private key

- As the Relying party for this CA is ČSOB itself, the potential internal mitigations must be considered before revoking the CA's Private key

- If the Private key is determined to be revoked, then the new Private key must be issued and the operation renew in the possible shortest time, and the new certificates issued with possible minimal impact, according to the analysis of mitigation procedures.

5.7.4 Business continuity capabilities after a disaster

The main components of the CA are operated in two different locations, which limits the probability of disaster. Also the key role of the CA Administrator is sufficiently staffed to ensure the business continuity of CA operation.

5.8 CA or RA Termination

In case the CA terminate its services, the subscribers must be notified in advance to ensure the smooth operation and the transition to some other service.

As the Relying party for this CA is the ČSOB itself, the trust for the CA Certificates must be ensured till the related services are provided or the other solution is in place to ensure the smooth operation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

All CA keys, which needs to be securely protected, are generated using FIPS validated HSMs. The key generation process is described in the internal operational documentation available to PKI Administrator role. The operational processes must be followed by PKI Administrator, and the four eye principle and the separation of roles is applied, where needed.

6.1.2 Private key delivery to subscriber

Not applicable.

6.1.3 Public key delivery to certificate issuer

The public key is delivered to the CA over encrypted channel, in signed PKCS#10 format.

6.1.4 CA public key delivery to relying parties

Not applicable.

6.1.5 Key sizes

The key size of the CA certificate, which is issued using RSA algorithm, is 4096 bits.

The key sizes of the certificates issued by CA according to this policy, issued using RSA algorithm, may be either 2048 bits or 4096 bits.

Besides that, all algorithms and key lengths are subject to internal ČSOB regulation of cryptographic algorithms and key sizes, and might be improved accordingly to address the new risks and to fulfil this internal regulation.

6.1.6 Public key parameters generation and quality checking

The keys should be generated according to the international standards and norms.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The following key usage is allowed for the corresponding Certificate:

EDSSCA Certificate - digitalSignature, keyCertSign.

EDSS Root CA Certificate - keyCertSign.

For the Certificates issued to Subscribers, the key usage is defined in the profile and is restricted to digitalSignature and keyEncipherement.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

To store the CA Private key, HSM is used, which fulfils the standard FIPS 140-2. The HSM are operated according to the internal operational documentation and operated only by PKI Administrators.

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

It is ensured only trusted personnel are required to act in order to access and use the CA’s Private Keys, including any Private Key backups and the four-eye principle is followed.

6.2.3 Private key escrow

Not applicable.

6.2.4 Private key backup

CA Private key is backed up in a separate HSM and stored in a secure location, different from the other HSMs used in operation.

The access to backup HSM is restricted to PKI Administrators.

6.2.5 Private key archival

CA Private key, which was replaced with the new one, are not stored or archived, and they are deleted.

6.2.6 Private key transfer into or from a cryptographic module

The transfer of the Private key is done only by PKI Administrators. The transfer is done only between HSMs via secure channel and the keys are never stored outside approved HSM.

6.2.7 Private key storage on cryptographic module

The CA Private Key is stored in HSM, which fulfils the standard FIPS 140-2, in a dedicated partition.

6.2.8 Method of activating private key

The activation of the Private key is done by PKI Administrator, according to the operational documentation, using native HSM functions.

6.2.9 Method of deactivating private key

Not applicable.

6.2.10 Method of destroying private key

The destroying/deletion of the private key is done by PKI Administrators, according to the procedures described in the operational documentation, via native functionalities of the HSM. Physical destruction of HW is not required.

6.2.11 Cryptographic Module Rating

See 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Public key of the CA is maintained during its validity and further archived by standard internal means till the end of internal PKI existence.

6.3.2 Certificate operational periods and key pair usage periods

Maximal date of operational period of the certificates (and the corresponding keys) is stated within each certificate, and defined for each type of the Certificate as follows:

CA Certificate – 20 years.

Root CA Certificate – 30 years.

For the Certificates issued to Subscribers, the operational period is defined by the CA configuration and set up to maximum 30 minutes..

6.4 Activation Data

6.4.1 Activation data generation and installation

The activation data for Private keys or HSM operation are generated either at HSM initialization or during Private key creation. They are maintained by PKI Administrators according to internal rules for sensitive information.

6.4.2 Activation data protection

The activation data are maintained by PKI Administrators according to internal rules for sensitive information, in combination of physical and logical access protection and encryption.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The computer security requirements and controls are defined by internal ČSOB rules and policies. For the CA, the specific requirements are described in technical documentation.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System development controls

The system development controls are defined by internal ČSOB rules and policies and following the practices of SDLC.

6.6.2 Security management controls

The security management are defined by internal ČSOB rules and policies and based on the international standard as ISO 27001.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network Security Controls

The network security controls are defined by internal ČSOB rules and policies following the best practices as usage of filtering devices on various levels of OSI layer model, network segmentation, etc.

6.8 Timestamping

Not applicable.

7. CERTIFICATE, CRL, AND OCSP PROFILE

7.1 Certificate Profile

7.1.1 Version number(s)

CA issues X.509 version 3 Certificates.

7.1.2 Certificate extensions

For issuing the Certificates to Subscribers, the following extensions are used:

- Authority Key Identifier
- Subject Key Identifier
- Authority Info Access (Policy Information)
- Netscape Comment
- Key Usage

7.1.3 Algorithm object identifiers

The algorithms used are designated in accordance with international standards and norms.

7.1.4 Name forms

For the profile used for issuing the Certificates to Subscribers, the following meanings of the names in the following parameters are used:

SERIALNUMBER – random generated number

UID – client identification (ICID)

PSEUDONYM – client identification (OLI number)

GIVENNAME – client first name

SURNAME – client last name

C – client certificate country

CN - client full name

O - organization name if specified

netscapeComment - configured text (template) with added algorithm and corresponding document fingerprint

policyInformation – OID and URI where this policy can be found

CertificateValidity – maximum 30 minutes or configuration parameter

keyUsage – set to digitalSignature a nonRepudiation

7.1.5 Name constraints

No stipulation

7.1.6 Certificate policy object identifier

Not applicable.

7.1.7 Usage of Policy Constraints extension

Not applicable

7.1.8 Policy qualifiers syntax and semantics

Not applicable.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL Profile

7.2.1 Version number(s)

Not applicable.

7.2.2 CRL and CRL entry extensions

Not applicable .

7.3 OCSP Profile

7.3.1 Version number(s)

Not applicable.

7.3.2 OCSP extensions

Not applicable.

8. COMPLIANCE AUDIT

The CA is audited within the general requirements for audit of the ČSOB, both by external audit and by internal audit, according to either regulatory requirements or according to internal rules for audit.

8.1 Frequency or circumstances of assessment

No stipulation, see 8.

8.2 Identity/qualifications of assessor

No stipulation, see 8.

8.3 Assessor's relationship to assessed entity

No stipulation, see 8.

8.4 Topics covered by assessment

No stipulation, see 8.

8.5 Actions taken as a result of deficiency

No stipulation, see 8.

8.6 Communication of results

No stipulation, see 8.

9. OTHER BUSINESS AND LEGAL MATTERS

Generally, the CP does not serve as a contract or a part of a contract. It is assumed that certain legal and liability terms and conditions will appear in separate documents and agreements with a subscriber, if needed.

9.1 Fees

There are no fees applied by CA to Clients.

9.1.1 Certificate issuance or renewal fees

Not applicable.

9.1.2 Certificate access fees

Not applicable.

9.1.3 Revocation or status information access fees

Not applicable.

9.1.4 Fees for other services

Not applicable.

9.1.5 Refund policy

Not applicable.

9.2 Financial Responsibility

Not applicable.

9.2.1 Insurance coverage

Not applicable.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

9.3 Confidentiality of Business Information

The confidential information are handled in compliance with internal ČSOB rules for classification of information.

9.3.1 Scope of confidential information

No stipulation, see 9.3.

9.3.2 Information not within the scope of confidential information

No stipulation, see 9.3.

9.3.3 Responsibility to protect confidential information

No stipulation, see 9.3.

9.4 Privacy of Personal Information

The personal information are handled in compliance regulatory requirements as GDPR, as well as in compliance with internal ČSOB rules which are aligned to external regulations.

9.4.1 Privacy plan

No stipulation, see 9.4.

9.4.2 Information treated as private

No stipulation, see 9.4.

9.4.3 Information not deemed private

No stipulation, see 9.4.

9.4.4 Responsibility to protect private information

No stipulation, see 9.4.

9.4.5 Notice and consent to use private information

No stipulation, see 9.4.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation, see 9.4.

9.4.7 Other information disclosure circumstances

No stipulation, see 9.4.

9.5 Intellectual Property Rights

No stipulation.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

CA asserts to provide the services accordingly in compliance with this CP and the internal rules and policies of ČSOB. This and all other representations and warranties individual or not to the specific business relationship are stipulated in the corresponding contract.

9.6.2 RA representations and warranties

Not applicable.

9.6.3 Subscriber representations and warranties

Not applicable.

9.6.4 Relying party representations and warranties

Not applicable.

9.6.5 Representations and warranties of other participants

Not applicable.

9.7 Disclaimers of Warranties

Except for statements explicitly present in this CP, or limited by law, all warranties and obligations related to this CP are disclaimed.

9.8 Limitations of Liability

Not applicable, see 9.

9.9 Indemnities

Not applicable, see 9.

9.10 Term and Termination

9.10.1 Term

This CP is effective since the date defined in table on page 2 with the history of changes and remain in effect until replaced with a newer version.

9.10.2 Termination

This CP and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of termination and survival

The stipulation in this CP are valid until they are replaced by new version of CP. The update of the CP takes into consideration the issued certificates and does not change the stipulation in a way that would influence the stipulation necessary for the already issued Certificates.

9.11 Individual notices and communications with participants

No stipulation

9.12 Amendments

9.12.1 Procedure for amendment

The amendments are made by CA Administrators and approved by the department manager.

9.12.2 Notification mechanism and period

The new version of CP is published internally and provided on request.

9.12.3 Circumstances under which OID must be changed

Not applicable.

9.13 Dispute Resolution Procedures

Not applicable, see 9.

9.14 Governing Law

Not applicable.

9.15 Compliance with Applicable Law

The CA is operated in compliance with applicable laws and international standards, if relevant.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

Not applicable.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

CA is not liable for a delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond CA’s reasonable control.

9.17 Other Provisions

No stipulation.