Public key infrastructure (PKI) in Komerční banka

Certification policy (CP)
for a
Subordinate certification authority of Komerční banka

Contents

1 Introduction

Certification policy defined for a subordinate certification authority provides a description and policy to be observed, including responsibilities of the parties concerned. The subordinate certification authority is included in the so-called ROOT CA KB tree; it follows its rules and, at the same time, allows for issue of certificates to users.

1.1 Terms used

The content of “Certification policy type” and “Certification implementation directive type” documents is based on the philosophy of the RFC2527 standard, where certification policy mostly documents the parameters of a certain certificate and its usability, unlike the directive, which primarily codifies procedures applied by individual bodies within the framework of PKI activities. There is no sharp division line set between the two document types.

Certification policy (CP) - rules defining the usability of certificates within the framework of individual groups and/or categories of applications in compliance with security requirements. These rules are supported by procedures defined in Certificate implementation directives (CPS).

Certification implementation directive (CPS) – creates a framework of rules defined by CP. In their procedures, provisions and regulations, these directives define the requirements for all PKI elements entering the registration and certification process. They specify details of one or more CP. In general, they contain the following:

- a list of Certification policies;
- for each CP: procedures, provisions and regulations defining how SC KB provides services resulting from CP;
- rules and procedures for issuing certificates and activities relating to certificates

Private key – data for creating a digital signature.

Public key – data for verifying a digital signature.

1.2 Abbreviations

CA	Certification authority
CP	Certification policy
CPS	Certification implementation directive
MRM	Local registration site
OMRM	Operator of a local registration site
PKI	Public Key Infrastructure
SC KB	Administration of certificates and public keys of KB; includes PKI administration teams
CS KB	KB certification service – includes all controlling, organisational and technological PKI structures
AP PKI	PKI application support
OID	Numerical object identifier used for identification of objects of a certain type within the framework of object classification according to ISO/ITU (within the certificate or other standardised data structure)
Root CA	Root certification authority (ROOT CA KB), the top of the certification authority tree

1.3 Identification

Document name:

Certification policy for a subordinate certification authority.

File name:

PKI_KB_Subordinate_CP_v101.doc

Identifier of this certification policy:

1.3.0154.45317054.31.1.45.3.0

This object identifier (OID) for object identification within the PKI infrastructure of Komerční banka is based on the basic KB OID derived from the international classification of the Czech Republic (1.3.0154…) from the ID of the organisation (IČO - 45317054).

The certification policy complies with CPS.

1.4 Applicability

1.4.1 Certification authority

This certification policy applies for a subordinate certification authority of KB - “DCS CA KB”. This certification authority is included in the certification tree; it does not allow further creation and support for its subordinate certification authorities.
A Subordinate CA can only issue certificates for clients/users.

1.4.2 Registration authority

This certification policy applies for technological registration authorities directly subordinate to DCS CA KB. From an organisational point of view, operators in local registration sites carry out registration operations. RA, OMRM and MRM are organizational parts of KB.

1.4.3 Inappropriate use

Using a Subordinate CA certificate is not appropriate in applications that are not able to verify the complete certification path.

2 Contacts

2.1.1 Contact persons

All questions and comments relating to this certification policy must be addressed to the OMRM branch or Liberec Call Centre.

2.1.2 Administration and management

This certification policy is administered via SC KB and administration is performed in line with chapter 8 CPS.

2.1.3 Departments responsible for CP in KB

SC KB is responsible for issuing and maintaining this CP.

3 General provisions

3.1 Rights, duties and commitments

3.1.1 KB

In special and exceptional cases, KB has the right to revoke/suspend the validity of a Subordinate CA certificate. All clients and administrators of Subordinate CAs must be informed immediately of such action. The certificate in question must be added to the list of revoked certificates (CRL) immediately.

3.1.2 PKI administration

SC KB registers requirements and approves/rejects requests for adding another subordinate certification authority to the KB certification authority tree according to the KB strategy.

3.1.3 Administration of certificates and public services of KB (SC KB)

SC KB is responsible for creating and possibly verifying the content of a request for issuing a certificate and for subsequent processing of that request according to principles and procedures defined in CP, CPS and related documents issued by KB. It keeps information on issued, suspended and revoked certificates according to appropriate provisions of CP and CPS, ensures data protection in compliance with the appropriate legal regulations and PKI security policy.
It informs and saves information stored in certificates of Subordinate CAs.

3.2 Guarantees

If KB issues a certificate through a CA, this means it guarantees that all procedures are performed in compliance with CP and CPS documents, that the certificate of the Subordinate CA is properly implemented and that name conventions comply with the requirements of policies and directives.

Komerční banka expressly rejects any guarantees that are not explicitly defined in CP.

3.3 Liability for damage

KB is responsible for running the PKI system and related structures via SC KB. KB is not responsible for improper usage of a certificate or key on the side of the client or the side that is dependent on the certificate.
If KB suffers losses, it will claim compensation by means of legal action.

3.4 Interpretation and enforcement of law

3.4.1 Governing law

Czech legal regulations will be considered authoritative and governing when claiming, interpreting and enforcing this CP and CPSs or the contracts in question.

3.4.2 Dissolution, merger with another entity, termination of activity

Procedures of SC KB comply with effective legal regulations of the Czech Republic. Every CS KB client will be informed of changes or termination of activity in time and in compliance with the rules defined by the appropriate legal regulations.

3.4.3 Resolution of disputes

Any dispute that cannot be settled in an amicable way will be subject to a legal decision. Legal proceedings will be held in the Czech Republic, in Czech.

3.5 Charges

No price for the subordinate certificate has been set.

3.6 Publishing information

SC KB publishes valid CP on its website. CPS is available upon written request, with the exception of sections relating to the security of the PKI system. After their validity expires, these documents will only be available in written copies subject to written request.
Certificate Revocation Lists are issued regularly every 6 hours and are available in the Public registry of certificates. KB uses HTTP and LDAP protocols to provide access to Certificate Revocation Lists.
The Root and Subordinate CA public key is published in the Public registry of certificates, where it is accessible via HTTP and LDAP protocols, and also on its web site, where it is accessible via HTTP(S) protocol. The Root and Subordinate CA certificate fingerprint is also published on this website.
SC KB will publish the Root and Subordinate CA certificate within the framework of its Public registry of certificates for a period of at least three years from the validity of all issued certificates expiring.
SC KB defines the extent of information to be published and procedures for publishing in CPS.

3.7 Verifying conformity

To ensure proper operation of all elements of SC KB, KB holds regular auditing of their operation. The auditor is a person independent of SC KB. At least once a year, CS KB must undergo a thorough (in-depth) audit with the participation of an external auditor (external to KB). KB shall set audit dates and appoint auditors.
Rules and procedures for auditing the conformity of real activities with documentation are defined in CPS.

3.8 Ensuring confidentiality

Information gained by SC KB (either in written or electronic form) in relation to a certificate request is properly archived and will not be abused. Procedures used are governed by the legal regulations of the Czech Republic.

3.9 Intellectual property rights

KB exercises intellectual property rights towards all CP and CPS documents.

4 Identification and authentication

4.1 Initial registration

See CPS or Contract for details.

4.1.1 Name conventions

The structure of name conventions is based on the X.500 standard. Compulsory certificate attributes of subordinate certification authorities are:
- Common Name (for entry of the name)
- Organisational Unit (for entry of information about the administrator)
- Organisation (for entry of the name of the organisation)
- Country (for entry of the country)

Common Name:	DCS CA KB
Organisational Unit:	PKI KB Executive
Organisation:	Komercni banka
Country:	CZ

4.1.2 Using name conventions

Data in the certificate request are defined in accordance with name conventions of KB and SC KB. Using a false name or pseudonym is not currently allowed.

4.1.3 Uniqueness of names

SC KB guarantees the uniqueness of names of Subordinate CAs.

4.1.4 Registered trademarks

KB is not responsible for verifying registered trademarks of applicants or third parties and does not perform such verifications.

4.1.5 Methods of proving private key ownership

All certificate requests must be signed using the private key related to its public key (such as using PKSC#10). This allows the CA operator to confirm and verify ownership of the private key and the validity of the filed request.

4.1.6 Verifying the identity of the applicant for a subordinate certificate

SC KB is obliged to confirm and verify whether the request complies with name conventions and with the required KB processes.

4.2 Regular renewal of keys

Certificates are valid for a period of 10 years. The next certificate is issued in such a way that its validity conforms to the Electronic Signature Act. Values in the certificate may vary according to KB requirements.

4.3 Replacement of a key after revocation

Identification and authentication after revocation of a certificate is performed in the same manner as in the initial registration.

4.4 Request for revocation/suspension of validity

A request for revocation shall be filed via the AP PKI team.

5 Operational requirements

Any details which may be required are stated in the CPS.

5.1 Certificate request

1) Preparatory process

The AP PKI team has prepared a document on name conventions of Subordinate CA and all available information:

- CP of Subordinate CA
- CPS of Subordinate CA
- Security policy of Subordinate CA

2) Registration, verification

Prior to the actual process, CA admin verifies all data, logs into the CA and checks the data in the certificate.

5.2 Issuing a certificate

After successful verification, the request will be confirmed and a certificate issued. CA admin will transfer the certificate to the Subordinate CA immediately, on the spot, and send the verification fingerprint of the certificate for publishing on the KB web server.

5.3 Acceptance of a certificate

Immediately after implementation in the Subordinate CA, SC KB considers the certificate accepted and usable.

5.3.1 Publication of a certificate

As soon as the certificate has been issued, it will be published in the publicly available registry of certificates. This registry is available according to the requirements and needs of electronic banking services, on the basis of exactly defined access methods.

5.4 Revocation and suspension of certificate validity

5.4.1 Circumstances for revocation/suspension of certificate validity

Certificate validity may be revoked or suspended in the following cases only:

- An authorised person asks for revocation/suspension of validity
- The private key of a Root CA has been compromised.
- The private key of a Subordinate CA has been compromised.

5.4.2 Who can ask for revocation/suspension of certificate validity

The AP PKI team will revoke/suspend certificate validity on the basis of a request from:

- Komerční banka – authorised persons;
- PKI administrator;
- Entities authorised by law.

5.4.3 Procedure when submitting a request for revocation of a certificate

a) Requests for revocation must be processed in writing and verified by SC KB.
b) Authorised persons may only ask for revocation of a certificate in person at a SC KB location.

5.4.4 Procedure when submitting a request for suspension of a certificate

a) Requests for suspension must be delivered in writing.
b) They must be verified by SC KB
c) Authorised persons may only ask for suspension of a certificate in person at a SC KB site.

5.4.5 Deadlines for revocation/suspension of certificate validity

After verifying the request, the certificate will be revoked by return. Suspension of the Subordinate CA certificate will be performed by return.
See CPS for details.

5.4.6 Verifying the validity of a certificate by dependent parties

Dependent parties are obliged to verify the validity of a certificate before using it. See CPS for possible methods of verifying validity (using CRL etc.).

5.5 Security audit procedures

CS KB defines events on the level of systems and provided services, which are recorded for the purpose of auditing. Recorded events are regularly (at least once a month) analysed and stored for at least 10 years from the date of their origin. Records are protected using a method appropriate to their sensitivity and importance.
See CPS for joint details of provisions and procedures for protection and processing of records for all relevant certification policies.

5.6 Archiving records

5.6.1 Archived records

CS KB particularly archives:
- information needed for auditing purposes,
- audit results,
- all exchanges of electronic messages between the client and PKI KB elements,
- current and previous versions of CP and CPS;
- migration protocols.
- signed registration forms and documents,
- written requests for revocation/suspension of certificate validity.

5.6.2 Period for storing records in archives

All archives will be stored for a period of 13 years.

5.6.3 Archive protection

Records are protected using a method appropriate to their sensitivity and importance. See CPS and internal regulations for details of procedures and provisions used.

5.7 Replacement of keys

5.7.1 Certification authority keys

The validity of old and new keys will overlap according to requirements of the Electronic Signature Act. For example, in case of a certificate of Subordinate CA valid for 10 years, a new certificate for the Subordinate CA will be issued three years before expiry of the validity of the certificate of the Subordinate CA and all newly requested certificates will be signed by the new one. This will prevent cases where a client's certificate is still valid but the CA's certificate is not. New certificates will be published on the KB website and in the Public registry of certificates.

5.7.2 Keys for cross certification of CS KB

CS KB cross certificates are, as with all other certificates, implemented via applicants. SC KB will inform applicants that the key will be replaced. The same procedures as in the initial cross certification must be undertaken.

5.8 Exposure and recovery after an emergency

See CPS and internal regulations for details of procedures and measures used.

5.8.1 Damage to information technology, software or data

Backups are the primary measure for recovery after damage to information technology or data.

5.8.2 Revocation of a public key

If the public key of an element that is part of CS KB is revoked, the following steps must be taken:
1. the CRL is updated and published,
2. the element is withdrawn from operation,
3. a new key pair is generated,

5.8.3 Exposure of a CS KB element's key

If a private key of an element that is a part of CS KB is damage/disclosed, the following steps must be taken:
1. the certificate is immediately revoked (see chap. 4.4),
2. all certificates issued under this key are revoked without delay,
3. the CRL is updated and published,
4. the element is deactivated,
5. an investigation is held to find the cause of the damage/disclosure in order to ensure that it can be avoided in the future,
6. a new key pair is generated.

All certificates issued before the key was impaired must be issued again.
KB bears all possible costs of issuing these.

5.9 Termination of CA activity

The activities of CS KB are, for example, bound with the services of Komerční banka, which use certificates. Therefore, operation of CS KB may only be terminated after timely notification of termination of operation. Clients will be informed of changes via the information channels of these services 3 months before termination of activity.

6 Physical, procedural and personnel measures

6.1 Physical security measures

Operation of the infrastructure of public keys requires thorough protection of key components. One important protection measure is physical security covering the following fields:
1. selection of suitable locations
2. protection of the location by technical means
3. restricted access – "regime" protection
4. distribution mains for utility networks and air conditioning
5. fire prevention measures

The Certification authority is installed in a location meeting the requirements for the highest level of security for its private key from the viewpoint of fire safety, regime protection and technical security. Access is continuously monitored and enabled for authorised specialists only.
Details of appropriate measures and procedures are defined jointly for all relevant certification policies in CPS and Internal security directives of PKI KB.

6.2 Procedural measures

Job contents within SC KB are assigned to several separate roles. Division of functions into different roles is based on the requirement of separating individual fields of activities to restrict system abuse. Individual functions can be divided between several employees.
Details of functions and roles are defined jointly for all relevant certification policies in CPS and Internal security directives of PKI KB.

6.3 Personnel measures

Cleared, trustworthy and reliable personnel are selected for work in SC KB. These employees are trained when they start working for SC KB. Training is updated regularly. If set principles and procedures are violated, the employee in question is sanctioned.
Details of personnel measures are defined jointly for all relevant certification policies in CPS and Internal security directives of PKI KB.

7 Technical security measures

7.1 Generating and installing key pairs

7.1.1 Generating keys

7.1.1.1 Keys for a certification authority

The following persons must be present during the process of generating keys for a Subordinate CA: PKI administrator, his deputy, AP PKI team worker, his deputy, members of the audit team and the manager responsible for the activities of SC KB. Key pairs are generated directly in the secured cryptographic module. Immediately after generation, a backup copy of the CA private key is created on a chip card. The card is stored in a secure location.

7.1.1.2 Keys for CA administrators

Generation of keys for a CA super admin (SCA) of a Subordinate CA is performed during the course of its initialisation or during the process of extension, as the case may be. Keys are protected by a password entered by the SCA. This SCA can change the password at any time. The PKI administrator has full rights and can generate keys for further admins (ACA) with various rights (auditor, operation monitoring or CRL issue).

7.1.2 Delivery of a public key of a Subordinate CA to SC KB

The public key is delivered within the framework of the certificate request. It is processed in the zone of the highest security level. SC KB accepts the certificate request in the PKCS#10 format. SC KB accepts only delivery in person to the SC KB workplace.

7.1.3 Distribution of a public key

The public key of a Subordinate CA is published as a part of the certificate in the Public registry of certificates of Komerční banka and also on the KB website http://www.mojebanka.cz. The Root and Subordinate CA certificate fingerprint is also published on this website.
The KB Root and Subordinate CA certificate fingerprint is part of the Contract for issuing and using the certificate.

7.1.4 Sizes of keys

A Subordinate CA key uses the RSA algorithm and has a length of 2048 bits.

7.1.5 Generating key content

Algorithms integrated in the SureWare Keyper cryptographic module are used for generating random numbers when generating keys of both Root CA and Subordinate CAs. This device meets level 4 of FIPS 140 – 1 standard for processes of key generation.

7.1.6 Restricting the usability of a certificate

A Subordinate CA certificate can only be used for signing public keys of clients/CA users and for issuing CRLs.

7.1.7 Using hardware and software equipment in the process of generating keys

A hardware cryptographic module is used for generating the CA key.

7.2 Protection of private keys

7.2.1 Cryptographic modules

To generate and store private keys of certification authorities, CS KB uses SureWare Keyper cryptographic modules that comply with FIPS 140 – 1 standard, level 4. The module is accredited by the responsible bodies of the Czech state administration.

7.2.2 Storing private keys

The private key of Root and Subordinate CAs is stored in the protected environment of the SureWare Keyper module.

7.2.3 Obligation to make private keys accessible

Clients' private keys generated by SC KB shall not be disclosed to any other entity.

7.2.4 Backup of private keys

Along with generating the key pair of the Subordinate CA, a backup of the private key is generated. During backing up, the key is encrypted by the module key and stored on a chip card. Cards are stored in a safe place.

7.2.5 Archiving private keys

See Internal security directives of PKI KB for the manner of archiving private keys used for operation of SC KB.

7.2.6 Activating a private key

The private key of the certification authority is only activated for the time the CS software is in operation. The conditions for activating the key are:

- unlocking the Keyper module keyboard (the module operator's key)
- activating module services (security administrator's chip card),
- entering passwords for the operating system, for the software of the certification authority and for the private key.

7.2.7 Deactivating the private key of the certification authority

The private key of the certification authority is deactivated at least in the following cases:

- the cryptographic module detected an attempt to violate security measures
- operation of the certification authority software using the private key is terminated. Only the SCA (CA super admin), ACA (CA admin), may perform deactivation subject to instruction issued by the Steering Committee.

7.2.8 Cancelling/deleting private keys

In case of a Subordinate CA, it is necessary to reset (zero) the cryptographic module and initialise chip cards with a backup key.

7.3 Other aspects of key administration

7.3.1 Archiving public keys (certificates)

Certificates are archived in a database for at least 13 years. This database is archived even after termination of the activities of the CA in such a way that the archiving term condition is met.

7.3.2 Period of validity of keys

The period of validity of a Root Certification authority key is 20 years.
The period of validity of a Subordinate CA is max.10 years.

7.4 Activation data

With a view to the frequency of use, passwords for access to modules, files or chip cards carrying private keys are stored in written form, in compliance with the regulations.
The interval and rules of obligatory change of passwords and the form of passwords are also specified in *the Internal security directives of PKI KB.*

7.5 Security of computer systems

During the course of designing the SC KB infrastructure, great emphasis was placed on thorough security of all components.
For the security measures of SC KB computer systems, including their networking, see *the Internal security directives of PKI KB*.

7.6 Security measures for lifecycle

Separating the design and development of PKI in KB from the production environment:

1. To design and develop the PKI system in KB, the testing and development environment is both physically and logically separated from the production environment.
2. New security elements, new operating systems, upgrades and updates are tested in this environment before implementing them in the production environment.

See the *Internal security directives of PKI KB* for details.

7.7 Security of networks

Technical administrators carry out regular checks and verifications of the condition and trafficability of networks within the KB structure.
See *the Internal security directives of PKI KB* for details.

7.8 Technical security of the cryptographic module

For implementation within the framework of CS KB, cryptographic modules must have a security level complying with the FIPS 140-1 standard, level 3. Cryptographic modules implemented in certification authorities must have a security level complying with the FIPS 140-1 standard, level 4.

8 Certificate profile and CRL

8.1 Certificate profile

A DCS CA KB certificate is a certificate linking a public key with a CA object. Certificates issued in compliance with this CP conform to the ISO 9594-8 (X.509) standard, version 3.

8.1.1 Registration process

SC KB will perform registration of Subordinate CAs in the location of implementation of the certificate of the Subordinate CA. Only after verification, will the request be passed on for certification to Root CA.

8.1.2 Certificate form

The following information is specified in the certificate:

- certificate version (version 3)
  - **2**
- CA name (Common Name attribute)
  - **DCS CA KB**
- Root CA administration name (Organisational Unit attribute)
  - **PKI KB Executive**
- organisation name (Organisation attribute)
  - **Komercni banka**
- country (Country attribute)
  - **CZ**
- key length
  - **2048**

- algorithm
  - **RSA**
- validity
  - **10** years
- usage of certificate (Key Usage extension)
  - **Digital Signature**
  - **Non-Repudiation**
  - **CRL Signing**
  - **Certificate Signing**
- identification of the Root CA public key (Authority Key ID extension)
  - **160-bit SHA-1 image of the certification authority public key**
  - **certification authority DN + certificate serial number**
- identification of certification subject public key (Subject Key ID extension)
  - **160-bit SHA-1 image of certification subject public key**
- object identifier of this certification policy (Policy OID extension)
  - **1.3.0154.45317054.31.1.45.3.0**
- location from which it is possible to download this certification policy (Policy OID extension qualifier)
  - **www.mojebanka.cz**
- certification policy document name (User Notice extension qualifier)
  - **Certificate Policy - Root Certification Authority**

8.1.3 Usability of the certificate

(See also 1.4) The certificate is used for digital signing (CRL and certificate). The certificate provides signing of public keys of clients/users.

8.2 CRL profile

CA supports the Certificate revocation list (CRL), version 2, available in the registry of certificates in compliance with DAP (LDAP) standard. As an alternative to CRL in LDAP, CS may use WEB servers or other services used for checking and verifying certificates.

8.2.1 CRL contents

CRL lists are issued with the following standard items (fields, attributes):
- signature algorithm
  - **sha1WithRSAEncryption**
- Issuer - has the same content as this attribute in the Root CA certificate
- time of issue of this CRL list (This Update)
- expected time of issue of the next CRL list (Next Update)

For version 2, issued CRL lists use the following extensions:
- alternative name of the certificate issuer (Issuer Alternate Name)
  - EmailAddress object
  - URI object
- identification of Root CA public key (Authority Key ID)
  - **160-bit SHA-1 image** of Root CA **public key**
- serial number of CRL list (CRL Number)

Issued CRL lists use the following parameters and items of revoked certificates:
- serial number of revoked certificate (Revoked Certificates)
- date and time of revocation (Revocation Date)
- reason for revocation (Reason Code)
  - this item is not compulsory; the reason need not be specified

9 Administration and specifications

9.1 Specifications of change and activity procedures

a) SC KB can only make corrective or editing changes without prior negotiations and approval (e.g. change to contacts or addresses). Other, significant changes relating to PKI elements in KB, their behaviour and rules must be approved by the Steering Committee using KB rules.
b) Notification shall be provided of errors, changes or expected changes to these documents to contact persons, or bodies specified in chap. 2.1.1 of this CP. This notification must also include a description of the change, reasons for the change and contact information for the person applying for the change.
c) SC PKI shall send all changes in CP issued within the changes in CP issued within the framework of the public key infrastructure to all relevant contact sites and have them posted there for a period of 1 month. Changes to the current CP will be distributed to the appropriate and responsible bodies by means of the Internet, Intranet and e-mail.
d) KB can accept, modify or reject proposed changes after these have been posted for the due period of time (1 month).
e) If the proposed changes to CP affect a certain number of users, KB can, within the scope of its exclusive rights, assign a new object identifier for the modified CP, supplement the existing CPS or create a new CPS.

9.2 Publishing and policy for notification of changes

9.2.1 Data not published deliberately in this CP

Instructions
Internal directives for SC KB operation,
Internal security directives of PKI KB

9.2.2 Distribution of defined CP and CPS

CP are distributed in the following ways:
- via the website: http://www.mojebanka.cz

CPS can be viewed:
- subject to written request at the registration site

Information on processes relating to CS KB security will not be provided.

9.3 CP approval processes

SC KB is responsible for preparing and approving documents.