Public key infrastructure (PKI) in Komerční banka

Certification policy (CP)
with a high level of personal identity verification of the applicant/client

Personal certificate on a chip card

Contents

1 Introduction

This certification policy with stated methodology for issuing certificates with a high level of client verification provides a description of registration, verification, certificate use and also principles to be observed, including the scope of responsibilities of the parties involved.

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.

Client – a natural person or legal entity concluding a contract with KB. They participate in the registration process, ask for issue of a certificate and their identity is verified. They own a private key and the corresponding certificate. They are responsible for protection and usage of the private key and the corresponding certificate.

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
ČK	Chip card
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
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)
CS	KB certification service – includes all management, organisational and technological structures

1.3 Identification

Document name:

Certification policy for a personal certificate issued on a chip card with a high level of identity verification.

File name:

PKI_KB_CP_E_Os_vys_cip_cl_v501.doc

Identifier of this certification policy:

1.3.0154.45317054.131.1.25.0.3

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.

Important notice for participants in the registration and certification process who are to use the methodology:

Clients are obliged to familiarise themselves with this Certification policy and corresponding CPS before they use certificates with high level of identity verification for the first time.

1.4 Applicability

1.4.1 CA

This certification policy applies for the external certification authority of KB – “DCS CA KB”. This certification authority is included in the KB certification tree whose root is the root KB certification authority – “Root CA KB”. DCS CA KB does not create or support subordinate certification authorities.

1.4.2 RA

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

1.4.3 Clients

Only a natural person who is competent of performing legal acts and whose identity can be verified can become a client.

1.4.4 Suitable applications

The following applications are recommended and tested for using this type of certificate (see also 7.1.3):

- electronic banking systems – supplied or implemented by Komerční banka, e.g. using the environment of a WEB browser (Internet banking) or an in-house KB application.
- verification of user identity – using a SSL protocol, e.g. WEB browser (Internet
- Explorer, Netscape Navigator) or so-called remote access client (VPN)
- e-mail environment can also be used – Outlook, Exchange, on its own or via supplied modules for securing e-mail.

1.4.5 Unsuitable applications

All applications not approved by this CP are considered unsuitable.

1.5 Contacts

1.5.1 Contact persons

All questions and comments relating to this certification policy must be addressed to OMRM, which will provide the required information.

1.5.2 Administration and management

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

1.5.3 Departments responsible for CP in KB

The PKI administrator is responsible for issuing and maintaining this CP.

2 General provisions

2.1 Rights, duties and commitments

Komerční banka

In special cases, SC KB has the right to revoke/suspend the validity of a client’s certificate. The client must be informed immediately of such an action and the certificate must be added to the certificate revocation list (CRL) immediately.

Certification authority

This issues certificates of PKI entities and clients according to principles and procedures defined in CP, CPS and related documents issued by KB, keeps information on issued, suspended and revoked certificates in compliance with appropriate provisions of CP and CPS and ensures data protection according to the appropriate legal regulations.

Registration authority

This registers applicants/clients and submits their certificate requests for processing in compliance with the principles and procedures defined in CP, CPS and related documents issued by KB.

Certificate holder (Client)

Uses the issued certificate only in compliance with this CP and related documents issued by KB; ensures protection of their private key according to appropriate provisions of CP and CPS and the Contract, as the case may be.

Dependent party

Verifies the validity of the certificate every time it is used.

Register of certificates

Provides clients/applicants and dependent parties with information stored in certificates and about suspension or revocation of the certificate according to the appropriate provisions of CP/S.

2.2 CA and RA guarantees

Certification authority

By issuing a certificate through CA, KB guarantees that all procedures are carried out in compliance with CP and CPS documents and that the certificate (client’s public key) is related to the client.

Registration authority

All procedures of the client’s/applicant’s registration comply with the appropriate CP, CPS and corresponding documents issued by KB.

Komerční banka expressly refuses any guarantees that are not explicitly defined in CPS.

2.3 Liability for damage

KB is responsible for running the PKI system and SC KB activities. 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.

See CPS for details about financial responsibility.

2.4 Interpretation and enforcement of law

2.4.1 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.

2.4.2 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.

2.4.3 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.

2.5 Charges

Certificate prices, if applicable, are published in the official certificate price list. The price list can be found on the KB web site. It can also be sent subject to request.

2.6 Publishing information

KB publishes valid CP on its web site. In addition, a printed copy of these documents is available subject to written request. After their validity expires, these documents will only be available in written copies subject to written request made at the OMRM branch.
Some parts of CPS are subject to rules of sensitive information; therefore, these will not be included in published documents. CPS can only be obtained subject to written request submitted at an OMRM branch.
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.
Root and Subordinate CA public keys are published as a part of the CA certificate in the Public registry of certificates, where they are accessible via HTTP and LDAP protocols, and also on the KB web site, where they are accessible via HTTP(S) protocol. Root and Subordinate CA certificate fingerprints are also published on this web page.
Root CA and Subordinate CA certificate fingerprints are parts of the Contract for issuing and using the certificate.
SC KB will publish the certificate of the KB Certification service 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.
KB defines the extent of information to be published and procedures for publishing in CPS.

2.7 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, SC 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.

2.8 Ensuring confidentiality

Information learnt by SC KB (either in written or electronic form) from clients in reference to their certificate request is properly archived and will not be abused. Procedures used observe the legal regulations of the Czech Republic.

2.9 Intellectual property rights

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

3 Identification and authentication

3.1 Initial registration

See CPS or Contract for details.

3.1.1 Name conventions

The structure of name conventions is based on the X.500 standard. Compulsory name attributes in the certificate are:

- Common Name (for entry of the holder’s/client’s name)
- Organisational Unit (for entry of the residency address and date of birth)
- Country (for entry of the country of residence)
- Locality (for entry of the town of residence)
- Subject Alternate Name-RFC822Name (for entry of e-mail address)

3.1.2 Using name conventions

Data in the application for a certificate are compared with the identification document.
Use of a pseudonym is not currently allowed.

3.1.3 Uniqueness of names

Registration sites cannot guarantee the uniqueness of names.

3.1.4 Name allegations, statements and doubts in the distinguishing procedure

These discrepancies will be resolved by SC PKI.

3.1.5 Registered trademarks

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

3.1.6 Methods of proving private key ownership

All electronic certificate requests must be signed by the client using his/her private key related to his/her public key (such as using PKSC#10). This allows the RM operator or PKI system to verify ownership of the private key.

3.1.7 Verification of the client’s identity

The RA is obliged to verify the applicant’s identity using procedures defined below in this CP or CPS. Prior to issuing a certificate with high level of client verification, the following information shall be verified (see chapter 4):

- country;
- town/municipality;
- street/place, number, postcode;
- client’s surname;
- client’s first name (and initials of other names, if applicable);
- year, month and day of birth;
- client’s contact e-mail address;
- contact telephone number;
- telephone number for sending one-off password via SMS.

Identification data of the client in the KB system is also added to the electronic certificate request and later to the certificate.
To verify the client’s identity, a valid identity document is required and possibly also an additional document, whereas documents with photographs are preferred.

3.2 Regular renewal of keys

Before expiry of the validity of the original certificate, the following takes place depending on the type of certificate.

a) The certificate request is signed with valid data for creating the digital signature. Data for verification of the digital signature will be changed, however, data leading to unique identification remain identical. A new certificate with a new period of validity will be issued. Verification of data for the unique identification will be carried out within the SC KB system.
b) If unique identification data for which identity documents must be shown are changed, the client’s participation in person in MRM is necessary. A new certificate will be issued after verification.

c) If a value other than values of unique identification is changed, such as an e-mail address, a new certificate can be issued on the basis of a delivered certificate request filled out with valid data for the creation of a digital signature. Data for creating a digital signature will be changed. Values of the unique identification must be identical with those specified in the personal submission of the request, with the exception of the e-mail address, for example. Unique identification values are compared with the values specified in the SC KB records.

3.3 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.

3.4 Request for revocation/suspension of validity

a) If a client or authorised third party requests revocation, the request must be confirmed with the following documents:
   - client – completed and signed form (request for revocation), identity will be verified according to a valid identity card. Before the request for revocation is sent, the password for certificate revocation/ suspension must be proven to be known;
   - authorised party - completed and signed form (request for revocation), identity will be verified according to a valid identity card and power of attorney. Before the request for revocation is sent, the password for certificate revocation/ suspension must be proven to be known;

b) If the client or authorised third party requests suspension of the certificate validity, this can be performed using the appropriate application, remotely, at the registration sites or via the Call centre.

3.5 Basic rules for work with ČK

SC KB guarantees that the basic criteria for work with ČK have been met:

a) keys are generated on ČK
b) the private key never leaves the ČK

4 Operational requirements

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

4.1 Certificate request

1) 1) Preparatory process

a) The client may copy and print appropriate files for the certificate of the highest level (Certification policy) from the KB website www.mojebanka.cz. The client can also pick up CP from the local registration sites of KB.
b) The client visits the local registration site in person with identity documents.

A meeting with an operator at a registration site can be arranged in advance. See www.mojebanka.cz for a list of local registration sites.

2) Registration, verification and handover of a one-off password at the registration site:

a) The local registration site (OMRM) operator hands over the ČK to the client. It is advisable to change the PIN. This can be performed before or after the process of issuing the certificate.
b) The local registration site (OMRM) operator verifies the client’s identity according to the identity card or additional document;
c) The OMRM processes data into the certificate request with the client;
d) Keys are generated in the presence of the client. The client confirms the displayed information by entering his/her PIN.
e) The OMRM provides the client with a printout of the approved certificate to check. If the client agrees with the data, he/she approves it and confirms his/her certificate application.

f) The OMRM prepares the contract on use of the certificate.

4.2 Issuing a certificate

After acceptance of a verified certificate application, SC KB generates the certificate and prepares it for collection. After acceptance (see chap. 4.3), the client then collects his/her certificate and imports it to the ČK.

4.3 Acceptance of a certificate

a) The whole process takes place at the registration site.
b) The certificate is considered accepted by the client and usable immediately after verifying the certificate using the application supplied by SC KB for certificate verification. The client is responsible for verifying the correctness of the certificate content. If the client finds any conflict between the data stipulated in the contractual agreement and the certificate content, he/she must immediately inform KB.
c) The OMRM revokes the certificate.
d) If the certificate is not verified, it is not considered accepted and usable.
e) If the certificate is not verified, the application may reject it.

4.3.1 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.

4.4 Revocation and suspension of certificate validity

4.4.1 Circumstances for revocation/suspension of certificate validity

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

- the client or an authorised person asks for revocation/suspension of validity;
- the certificate was issued on the basis of incorrect or false information or information on whose basis it was issued is no longer valid;
- the client (certificate holder) seriously breached the Contract;
- the CS KB private key has been compromised.

4.4.2 Who can ask for revocation/suspension of certificate validity

CS KB will revoke/suspend certificate validity on the basis of a request from:

- the client (certificate holder) or party authorised by them;
- the MRM operator who issued the certificate;
- SC KB;
- entities authorised by law.

4.4.3 Procedure when submitting a request for revocation of a certificate

a) Requests for revocation must be written, password-confirmed and then verified by SC KB.
b) The client must be verified by procedures of verification and confirmation of actual certificate ownership (see chapter 3.4).
c) The client/authorised party may ask for revocation of the certificate in the following ways:
    - in person – at the MRM with a request for certificate revocation, supplemented with the revocation password for the certificate;
d) The client/authorised person may first ask for suspension of certificate validity by telephone, fax or electronic channel (see next chapter), with subsequent delivery of the request for revocation or cancellation of suspension.

4.4.4 Procedure when submitting a request for suspension of a certificate

a) The client/authorised person may request suspension of validity in the following ways:

- by telephone – with a request for suspension of validity,
- in person – with a request for suspension of the certificate, at the MRM,
- by fax – with a request for suspension of validity at the KB branch,
- by e-mail – with a request for suspension of validity to the OMRM,
- via the application created by SC KB and available on the Internet, supplemented with the certificate validity revocation/suspension password.

4.4.5 Deadlines for revocation/suspension of certificate validity

After verifying the request, the certificate will be revoked/suspended by return, no later than during the time limit set by SC KB.
See CPS for details.

4.4.6 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.).

4.5 Security audit procedures

SC 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 week) 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.

4.6 Archived records

4.6.1 Archived records

SC 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.

The MRM shall particularly archive written documents used within the framework of services via electronic distribution channels:

- signed registration forms - Contract on providing and using the certificate,
- written requests for revocation/suspension of certificate validity.

4.6.2 Period for storing records in archives

All archives will be stored for a period of 10 years.

4.6.3 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.

4.7 Replacement of keys

4.7.1 Users' keys

The client will be automatically be warned by e-mail 30 and 15 days before expiry of validity. The new certificate will not be automatically issued on the basis of previous data. The client must ask for a new certificate or prolongation of the certificate validity. It is recommended that all types of newly created certificates are based on new key pairs, since the period of the validity was set for security reasons.

4.7.2 Certification authority keys

Validity of old and new keys will overlap: the new key is issued three years and a month before the key validity expires, and all certificates newly applied for will be signed with the new certificate. 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.

4.7.3 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.

4.8 Exposure and recovery after an emergency

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

4.8.1 Damage to information technology, software or data

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

4.8.2 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.

4.8.3 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.

4.9 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.

5 Physical, procedural and personnel measures

5.1 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.

5.2 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.

5.3 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.

6 Technical security measures

6.1 Generating and installing key pairs

When defining requirements for cryptographic keys, two types of key owners must be distinguished:

- keys for internal use of SC KB, such as keys of certification and registration authorities,
- keys for clients.

6.1.1 Generating keys

6.1.1.1 Keys for a certification authority

The following persons must be present during the process of generating keys for Root CA KB and DCS CA KB: PKI administrator, his deputy, AP PKI team worker, his deputy, members of the audit team, external independent auditor 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.

6.1.1.2 Keys for other modules of Public key infrastructure in Komerční banka

Keys for Registration authorities and other modules of the Public key infrastructure in Komerční banka (RA, RAO, WebRAO, …) are generated by a member of the application support team for Public key infrastructure in Komerční banka in the presence of operators responsible for the appropriate modules for which the keys are generated. Keys are protected by a password entered by the operator. This operator can change the password at any time.

6.1.1.3 Generating keys for clients using their own facilities

The client is responsible for the process of generating key pairs and requests for the certificate on their HW (PC). Software supplied or recommended by SC KB can be used. The client is also responsible for safe storage of the private key. If generating the private key onto a file, it is recommended that it be saved outside of shared disks. Passwords/PIN ensuring access to the private key must not be stored in an open form or disclosed to other persons.

6.1.1.4 Generating keys for clients using SC KB facilities

Keys are generated by MRM operators in the SC KB environment on ČK using the appropriate technologies that meet OKCS standards and the principles of security**. Clients enter passwords/PIN ensuring access to the private key in person at the MRM**. It is advisable to change the PIN from your own HW after leaving the branch.

6.1.2 Handover of the client's private key

The client's private key is handed over:

- on a chip card protected with a password/PIN in PKCS#11 format.

6.1.3 Delivery of a client's public key to SC KB

Clients' public keys are delivered within the framework of the electronic certificate requests. SC KB accepts certificate requests in these formats: PKCS#10, PEM, REQ or DER. SC KB accepts the following modes of application delivery:

- during registration in person, in terms of generation of keys and electronic applications for a chip card.

6.1.4 Distribution of a public key (certificate)

6.1.4.1 Distribution of a CS public key (CS certificate)

The public key of the Root or subordinate CS is published as a part of the CS certificate in the Public registry of certificates of Komerční banka and also on the KB website http://www.mojebanka.cz. Certificate fingerprints are also published on this web page.
CS KB certificate fingerprints are parts of the Contract for issuing and using the certificate.

6.1.4.2 Distribution of a client's public key (client's certificate)

The client's certificate is published in the KB Public registry of certificates.

6.1.5 Sizes of keys

A certification authority key uses the RSA algorithm and has a length of 2048 bits.
Keys of other modules of the Public key infrastructure in Komerční banka use RSA algorithms of 2048 bits.
The minimum length of a user's key is 1024 bits. Users may use the RSA algorithm for signature.

6.1.6 Generating key content

Algorithms integrated in the cryptographic module are used for generating random numbers to generate CA keys. The process of key generation is certified on this device, too.
When generating keys for other PKI KB modules and clients, mouse movements and keyboard activities are scanned for a time period to initially set the random number generator.

6.1.7 Restricting the usability of a certificate

Certificates issued by SC KB contain extensions modifying the manners of using these certificates in compliance with X.509v3.
Certificates issued according to this CP can only be used for the following purpose:
- encryption, decryption, digital signature and for non-repudiation.

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

6.1.8.1 CA

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

6.1.8.2 PKI core

Keys for certification authority users are generated on a chip card, in a protected file.

6.1.8.3 Client

Keys for clients are generated in a PKCS#11 type file on a ČK.

6.2 Protection of private keys

6.2.1 Cryptographic modules

To generate and store private keys of certification authorities, SC KB uses SureWare Keyper cryptographic modules that comply with FIPS 140 – 1 standard, level 4.
For the core of the Public key infrastructure in Komerční banka, chip cards are also used for protection of private keys. These cards not only allow safe storage of the key but also generation of keys within cards.

6.2.2 Storing the private key

Only the backup private key of the certification authority is divided into two parts and saved on two chip cards. Both cards are stored in a protected room with controlled physical access.
Logical access to cards is password-protected, while each of the two SC KB team members knows the access password to only one card.
The client's private key is stored on a ČK and never leaves this ČK.

6.2.3 Obligation to make private keys accessible

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

6.2.4 Backup of private keys

Along with generating the key pair of the certification authority, a backup of the private key is generated. When creating the backup, the key is divided into two chip cards (see 6.2.2).
SC KB does not provide backup of clients' private keys.

6.2.5 Archiving private keys

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

6.2.6 Activating a private key

The private key of the certification authority is only activated for the time the CS software is in operation. The following conditions must be met to activate the key: passwords entered for the operating system, for CA software and for private key entered concurrently by two persons.
The private key of the client is only activated for the period the client application that uses it is in operation. A condition for activating the key is entry of the password/PIN.

6.2.7 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) or ACA (CA admin) may perform deactivation subject to instruction issued by the Steering Committee.

6.2.8 Cancelling/deleting private keys

In the case of a certification authority, it is necessary to reset (zero) the cryptographic module and initialise chip cards with a backup key. For other elements of the Public key infrastructure in Komerční banka, only chip cards containing their private keys are initialised.

In case of PKI core, only a SCA (CA super admin) or ACA (CA admin) can execute deactivation.
Cancellation of the client's private key is performed by the client by destroying the chip and immediate revocation of the certificate.

6.3 Other aspects of key administration

6.3.1 Archiving certificates (public keys)

Certificates (public keys) are archived in a CS database for at least 10 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.

6.3.2 Period of validity of keys

The period of validity of a Certification authority key is 10 years.
The period of validity of a client certificate and the corresponding private key is 2 years.

6.4 Activation data

Passwords entitling access to files or chip cards with private keys for Public key infrastructure in Komerční banka modules are stored in written form, according to Internal security directives of PKI KB.
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*.

6.5 Securing 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.*

6.6 Security measures for lifecycle

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

- To design and develop the PKI system in KB, the testing and development environment is both physically and logically separated from the production environment.
- Only the PKI administrator, members of the PKI application support team and test specialists have access to this environment.
- New security elements, new operating systems, upgrades and updates are tested in this environment before implementing them in the production environment.
- New security elements, new operating systems, upgrades and updates are tested in this environment before implementing them in the production environment.
- See *Internal security directives of PKI KB* for details.

6.7 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.

6.8 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.

7 Certificate profile and CRL

7.1 Certificate profile

A certificate with high level of identity verification is a certificate linking a public key to the client. It is a personal certificate ensuring a strong guarantee of the relationship between the personal identity of the client and the public key. Certificates issued in compliance with this CP conform to the ISO 9594-8 (X.509) standard, version 3.

7.1.1 Registration process

Registration of certificates of the highest level is carried out at local registration sites (MRM) by operators of these sites (OMRM).
The client visits the KB registration site, proves his/her identity at the MRM (see 4.1, 4.2 and 4.3).

7.1.2 Certificate form

The following information is specified in the certificate:
- certificate version (version 3)
    - **2**
- name, surname and title where applicable (Common Name attribute)
- date of birth in the format YYYYMMDD (Organisational Unit attribute)
- place of residence – town/municipality (Locality attribute)
- address – street, number (Organisational Unit attribute)
- e-mail address (RFC822Mailbox extension)
- key length
    - **1024**
- algorithm
    - **RSA**
- validity
    - **2 years**
- usage of certificate (Key Usage extension)
    - **digital signature**
    - **encryption**
    - **authentication**
- identification of DCS CA public key (Authority Key ID extension)
    - **160-bit hash of public key of the certification authority**
    - **certification authority DN + certificate serial number**
- identification of certification subject public key (Subject Key ID extension)
    - **160-bit hash of public key of the certificate subject**
- object identifier of the security policy (Policy OID extension)
    - **1.3.154.45317054.131.1.25.0.2**
- location from which it is possible to download this Certification policy (Policy OID extension qualifier)
    - **www.mojebanka.cz**
- customer's identifier - client's identifier (generic extension, OID)
    - **1.3.0154.45317054.1.4.0**
    - parameter = numeric value

7.1.3 Usability of the certificate

(See also 1.4) The certificate is used for digital signature, data encryption and authentication.
The certificate ensures a high level of identity verification. Therefore, it can be used in applications securing banking operations of the appropriate level. It ensures encryption or authentication and ensures banking transactions via a digital signature. It can, for example, be used for electronic or business contact with Komerční banka, a.s.

7.2 CRL profile

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

7.2.1 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 DCS 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 the DCS CA public key (Authority Key ID)
  - **160-bit hash of the DCS SA 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

8 Administration and specification

8.1 Specifications of change and activity procedures

a) SC PKI 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 and processes.
b) Notification shall be provided of errors, changes or expected changes to these documents to contact persons, or bodies specified in chap. 1.5 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 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.

8.2 Publishing and policy for notification of changes

8.2.1 Data not published deliberately in this CP

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

8.2.2 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.

8.3 CP approval procedures

SC PKI is responsible for preparing and approving documents.