COMMERZBANK - X.509 PKI

COMMERZBANK PERSONS PKI

Certificate Policy (CP)

&

Certification Practice Statement (CPS)

Edition 1.0

Document Control:

Title:	Commerzbank Personen PKI – Persons PKI Certificate Policy (CP) & Certification Practice Statement (CPS)
Description:	Illustration of processes and procedures of the Commerzbank Persons PKI
RFC Schema:	RFC 3647 (Certificate Policy and Certification Practices Framework)
Authors:	Ralf Baumgart, Commerzbank AG, GS-ITR 4.3.5 Jung-Uh Yang, Consultant

Revision Control:

Edition	Date	Comment
1.0	01.02.2011	Final Version V. 1.0

Contents

1. Introduction

The term “Certificate Policy” (CP) is defined in the X.509 standard and means the whole set of rules and specifications, which define the applicability of a certificate type. The aim of a Certificate Policy is discussed in detail in RFC 3647 (“Certificate Policy and Certification Practices Framework”). The CP helps the subscriber in deciding, if a certain certificate or application can be trusted.

A CP should explain:

- Important technical and organizational requirements that have to be fulfilled by systems and processes when issuing certificates.
- Which prerequisites apply when using certificates and dealing with the corresponding keys and signature creation units (e.g. Smart Cards).
- Which meaning the certificates and the related applications have, e.g. which importance, evidentiary value, and legal pertinence the cipher text and signatures have that have been created using the certificates.

The concept of a “Certification Practice Statement (CPS)” was developed by the American Bar Association (ABA) and is quoted in their Digital Signature Guidelines (ABA Guidelines). The CPS is a detailed description of the certification operations of the organization. For this reason, organizations running one or more certificate authorities, usually also provide a CPS. As part of a company-wide PKI, the CPS is an adequate means for organizations to protect themselves, as well as to illustrate commercial transactions with certificate owners and relying parties.

A central aspect of the Commerzbank CP/CPS for the Commerzbank Personen PKI is the determination of the trustworthiness of issued certificates and the certificate operation, operated by the Commerzbank data center. By participating in the Commerzbank certification services, the Commerzbank employees and relying parties accept the terms and conditions listed in the CP/CPS.

The document structure is based on the recommendations of RFC 3647. According to the provisions of RFC 3647, the Commerzbank CP/CPS of the Commerzbank Personen PKI describes the procedures that are applied by the certification service on certificate application, generation, issuance and management.

Due to the requirements of a simplified document mananagement, the CP (Certificate Policy) and the CPS (Certification Practice Statement) have been combined in a central document. This document is free of charge and publicly available.

1.1. Overview

A central aspect of the Commerzbank CP/CPS for the Commerzbank Personen PKI is the determination of the trustworthiness of issued certificates and the certificate operation, operated by the Commerzbank data center. By participating in the Commerzbank certification services, the Commerzbank employees and relying parties accept the terms and conditions listed in the CP/CPS.

The document structure is based on the recommendations of RFC 3647. According to the provisions of RFC 3647, the Commerzbank CP/CPS of the Commerzbank Personen PKI describes the procedures that are applied by the certification service on certificate application, generation, issuance and management.

Due to the requirements of a simplified document mananagement, the CP (Certificate Policy) and the CPS (Certification Practice Statement) have been combined in a central document. This document describes the certification policy and the certification services operation of the Commerzbank AG X.509 – Personen PKI solution. It is free of charge and publicly available for Commerzbank employees.

1.1.1. Commerzbank Personen PKI architecture

The Commerzbank AG operates certification services to create, issue and manage certificates. The Commerzbank PKI allows the controlled issuance of certificates and smart cards.

Commerzbank users receive certificates and smart cards controlled and managed by a certificate and smart card management system. Commerzbank smart card certificates and certificates for group mail boxes/resource mail boxes are requested by the Personen PKI on behalf of the Commerzbank applicants.

Furthermore CA certificates are issued to certify the root CA **Commerzbank AG Inhouse Root CA** and the subordinate **Commerzbank AG Inhouse Sub CA 03**.

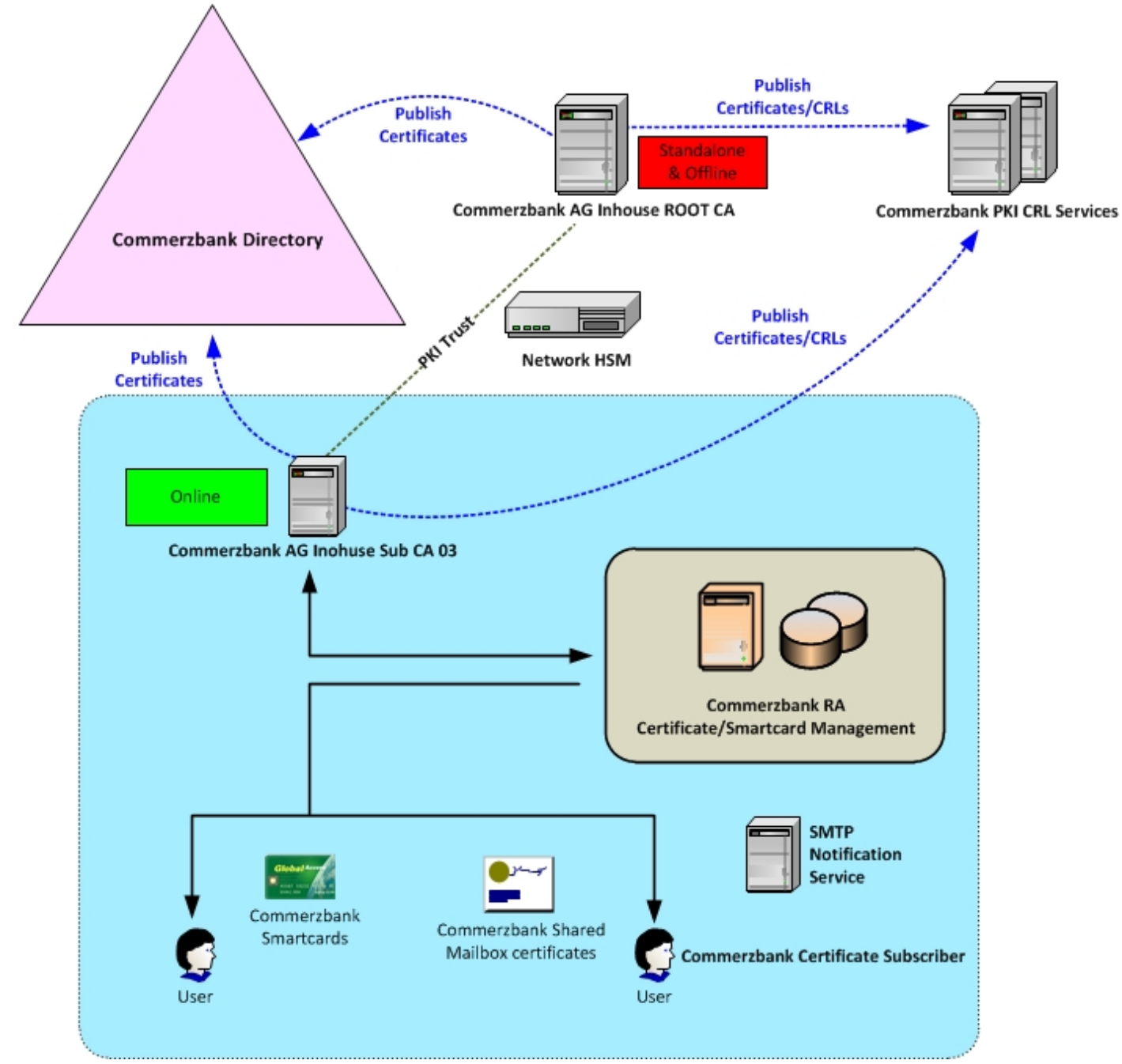
A network hardware security module (HSM) generates and manages keys for the Commerzbank CAs and the certificate management.

The Commerzbank certification infrastructure is designed hierarchically and terminates at the **Commerzbank AG Inhouse Root CA**. Further information about the architecture of the Personen PKI can be requested. Find contact information in chapter 1.5.2. “Contacts”.

Note: There is another CP/CPS documentation about the Commerzbank Inhouse Gateway CA. As Commerzbank Personen PKI and Commerzbank Gateway PKI both terminate at the Commerzbank AG Inhouse Root CA, this root CA is mentioned in both CP/CPS documentations.

In the Commerzbank PKI environment more CAs are established. However, these have no outreach. Hence, these CA components are not mentioned in the current CP/CPS documentations for the Commerzbank Gateway PKI or the Commerzbank Personen PKI.

Commerzbank Personen PKI



1.2. Document name and identification

This is the Commerzbank AG *"Certification Practice Statement and Certificate Policy"* of the Commerzbank Personen PKI. A unique ASN.1 Object Identifier (OID) is assigned to this document.

The Commerzbank OID is registered at IANA.ORG, see:

http://www.iana.org/assignments/enterprise-numbers

Commerzbank Enterprise OID: 1.3.6.1.4.1.14978

OID Description: Commerzbank SMI Network Management
Private Enterprise Code

Commerzbank PKI OID: 1.3.6.1.4.1.14978.5

OID Description: Namespace of the X.509 PKI services of Commerzbank AG

The CP/CPS title is:

Commerzbank Personen PKI – Certificate Policy (CP) & Certification Practice Statement (CPS)

Commerzbank CP/CPS OID: 1.3.6.1.4.1.14978.5.1

OID Description: OID of the Commerzbank AG Certificate Policy & Certification Practice Statement documentation

Commerzbank CP/CPS OID: 1.3.6.1.4.1.14978.5.1.3

OID Description: OID of the Commerzbank Personen PKI –
Certificate Policy & Certification Practice Statement

The location of the Commerzbank AG CP/CPS documentation for Commerzbank subscribers and trusted parties is: http://ca.commerzbank.com/cps/cps.htm

The Commerzbank operates the CAs in a 2-tier-architecture. The unambiguousness of the CAs is ensured by the CA's "Distinguished Name".

The complete DN of the Commerzbank Inhouse Root CA reads:

- **Commerzbank AG Inhouse Root CA**

  CN=Commerzbank AG Inhouse Root CA,

  O=Commerzbank AG,

  L=Frankfurt am Main,

  C=DE

The complete DN der Commerzbank AG Sub CA 03 reads:

- **Commerzbank AG Inhouse Sub CA 03**

  CN=Commerzbank AG Inhouse Sub CA 03,

  O=Commerzbank AG,

  L=Frankfurt am Main,

  C=DE

1.3. PKI participants and instances

The participants of the Commerzbank Personen PKI are classified in four participant groups. Each group offers PKI services and resources or consumes PKI services and resources.

Certificate Authority (CA):

- Issuing certificates;
- Revoking certificates;
- Recover user keys.

Registration Authority (RA):

- Identification of users and machines;
- Registration of users and machines;
- Applying for a certificate on behalf of other users;
- Applying for a certificate revocation.

Certificate users:

- Konsumiert Zertifikate und PKI Dienstleistungen

Relying parties (e.g. e-mail recipients):

- Consumes PKI services

1.3.1. Certificate authorities

The 2-tier CA hierarchy model is based on:

- ***Offline Commerzbank AG Inhouse Root CA*** with self-signed CA certificate. The Commerzbank Root CA is decoupled from the productive network and has a dedicated connection to the Network Hardware Security Module (HSM). All cryptographic operations of the Commerzbank Root CA are performed by the HSM.
  The Commerzbank Root CA issues CA certificates and revocation lists for subordinate certification instances (Commerzbank AG Sub CA) and for own use.
- ***Online Commerzbank AG Inhouse Sub CA 03*** with certificate issued by the Commerzbank Root CA. The Commerzbank AG Inhouse Sub CA 03 is connected to the productive network and has a dedicated connection to the Network HSM, like the Commerzbank Root CA. All cryptographic operations of the Commerzbank AG Inhouse Sub CA 03 are performed by the HSM. The Commerzbank Sub CA 03 issues end-entity certificates (for Commerzbank smart cards and Commerzbank group mail boxes) and revocation lists for subscribers.

Following life spans are defined for the Commerzbank AG certificate authorities:

Commerzbank AG Inhouse Root CA

- Root CA certificate: 30 years
- Root CA CRLs: 4 years

Commerzbank AG Inhouse Sub CA 03

- Sub CA 03 certificate: 10 years
- Sub CA 03 CRLs: 14 years

1.3.2. Registration authorities

The registration authorities in terms of this Certificate Policy are instances which register and identify subscribers and applicants and apply for certificates on behalf of subscribers. The registration of employee certificates is performed in local registration authorities (LRA). Those support the certificate operations of the X.509-based PKI. The central task is the provision of external user certificates for the communication with relying parties.

The certificate application for subscribers is performed via a registration tool that allows a controlled issuance of certificates on smart cards. Furthermore, the complete life cycle management of certificates is performed with this tool. The initial application is not performed by the subscribers.

1.3.3. Certificate users

Certificate users are end-entities which are assigned a certificate by the Commerzbank Inhouse Sub CA 03. Key generation and certificate issuance are not controlled by the subscriber, but by the Personen PKI.

End-entities as subscribers in terms of this PKI are Commerzbank full- and part-time employees, technical systems (like a mailbox for a web application) and, if needed, also business partners and external staff, which are assigned a S/MIME certificate by the Personen PKI.

1.3.4. Relying parties

Relying parties in terms of this Certificate Policy are all persons and systems that want to communicate securely with a certificate owner, using the certificate. In general, relying parties are recipients of S/MIME-secured e-mail messages. Relying parties are no Commerzbank employees or participants which have received certificates or smart cards from Commerzbank.

1.3.5. Other participants

Not applicable.

1.4. Certificate usage

The use of keys and certificates rests with the responsibility of the subscriber and the relying party.

1.4.1. Appropriate certificate uses

The smart card certificates issued under this CP/CPS can be used for **authentication** (e.g. Windows logon) and for ***encryption and signature***.

In case of group mail boxes, the certificates are only used for e-mail **encryption**.

The following table describes appropriate certificate uses:

Issued by Commerzbank AG Inhouse Root CA:

Certificate Type	**Appropriate Certificate Use**
Certificate Authority	ROOT CA Zertifikat for self-signed (root-)CAs

Issued by Commerzbank AG Inhouse Root CA:

Certificate Type	**Appropriate Certificate Use**
Subordinate Certificate Authority	CA certificate for subordinate CAs

Issued by Commerzbank Inhouse Sub CA 03:

Certificate Type	Appropriate Certificate Use
Coba SC Authentication	Smart card authentication certificate for logon, e.g. Windows logon
Coba SC Encryption	Smart card encryption certificate for encryption, e.g. e-mail encryption
Coba SC Signature	Smart card signature certificate for electronic signature, e.g. e-mail signature
Commerzbank Soft PSE Encryption	Software encryption certificate for e-mail encryption for group mail boxes
"Zertifikate für das Zertifikatsmanagmentsystem" (Certificate for certificate management system)	Additional software certificates were created for the operation of the certificate management system. These certificates are designed for technical use within the system.

1.4.2. Prohibited certificate uses

The use of user certificates in the scope of the Commerzbank Personen PKI is limited to:

- Authentication
- Encryption
- Electronic signature

The use of CA certificates in the scope of the Commerzbank Personen PKI is limited to:

- Signature of CA certificates for the Commerzbank Inhouse Root CA
- Signature of end certificates for the Commerzbank Inhouse Sub CA 03

Private use of certificates is prohibited as well as other use of these certificates except the authorized certificate uses as stated in 1.4.1. appropriate certificate uses.

Every other certificate use is prohibited, especially the certification of further, subordinate CAs is limited to the Commerzbank Inhouse Root CA, as well as the use of Commerzbank certificates for the qualified electronic signature.

To protect the Commerzbank CP/CPS conformity every change or extension of certificate uses has to be reported to the Commerzbank PKI Administration immediately.

1.5. Policy administration

1.5.1. Organization administering the document

The Commerzbank AG is the responsible organization, administering the policies.

Commerzbank AG
60261 Frankfurt am Main
Deutschland

1.5.2. Contact person

The following person is the contact for the Commerzbank Personen PKI:

Ralf Baumgart
Commerzbank AG
GS-ITR 4.3.5
Commerzbank AG
Mainzer Landstr. 151
D-60261 Frankfurt am Main
Tel.: + 49 69 13640448
Fax: + 49 69 13624280
Mobile: + 49 172 6929073
E-Mail: ralf.baumgart@commerzbank.com

1.5.3. Person determining CPS suitability for the policy

The Commerzbank AG, GS-ITR 4.3, is responsible for compliance with certification operation and policies according CP/CPS and supplementary documentation. Compliance contacts for CP/PS are listed in 1.5.2. contact person.

1.5.4. CPS approval procedures

The Commerzbank AG, GS-ITR 4.3, is responsible for release of this CP/CPS. The CP/CPS documentation is continuously being monitored for conformity.

1.6. Definitions and acronyms

ABA (American Bar Association) – Association of American auditors

ASN.1 (Abstract Syntax Notation) – Abstract Syntax Notation No. 1, data description language

C (Country) – Country object (Part of X.500 Distinguished Name), for Germany: C=DE

CA (Certification Authority)

CN (Common Name) – Name object (Part of X.500 Distinguished Name)

CP (Certificate Policy)

CPS (Certification Practice Statement) – Certification operation

CRL (Certificate Revocation List) – List of certificates, which are revoked but not expired yet, issued by the certificate issuing authority

CSR (Certificate Signing Request) – Signed certificate request

DN (Distinguished name) – Distinguished Namem, based on X.500 naming scheme

DNS (Domain Name System) – Standard for Internet names

FIPS (Federal Information Processing Standard) – US governmental encryption standard

HSM (Hardware Security Module) – Hardware component, that securely processes and stores security relevant information like data and cryptographic keys

IETF (Internet Engineering Task Force) – Task force for technical development of the Internet. Specifies quasi-standards as RFCs.

IP (Internet Protocol)

ISO (International Organization for Standardization)

ITU (International Telecommunications Union) – Standardization organization, specified X.509

LDAP (Lightweight Directory Access Protocol)

NIST (National Institute of Standards and Technology) – Standardization instance of the U.S.

O (Organization) – Organization object (Part of X.500 Distinguished Name)

OID (Object Identifier) – Distinct reference for objects in the OID namespace

OU (Organizational Unit) – Organizational unit object (Part of X.500 Distinguished Name)

PIN (Personal Identification Number) – Secret number for authentication of individual against e.g. a smart card

PKCS (Public key Cryptographic Standard) – Series of quasi-standards for cryptographic operations, specified by RSA

PKI (Public Key Infrastructure) – Description of technology, resources and participants in scope of asymmetric cryptography

PKIX (Public Key Infrastructure eXchange) – Series of specifications of the IETF concerning digital certificates according to X.509

RA (Registration Authority)

RFC (Request For Comment) – Quasi-Internet-standard, issued by IETF

URL (Uniform Resource Locator) – Resource location in the Internet

X.500 – Protocols and services for ISO-conformal directories

X.509 – Authentication method for X.500 directories

X.509v3 – Current PKI certification standard

2. Publication and repository responsibilities

2.1. Repositories

The Commerzbank Personen PKI uses its internal directory services for secure e-mail communications. The required receiver certificates are managed by the Personen PKI.

For public information like Commerzbank CA certificates, CRLs, and CP/CPS documentation a web based information service is used. CA information, except the CP/CPS documentation, is also published in the Commerzbank directory service.

2.2. Publication of certification information

The publication of encryption certificates (certificates of e-mail recipients) into the local directory service is carried out automatically by the Personen PKI. No user intervention is necessary. External recipient certificates for secure e-mail communications are provided by an upstream exchange of recipient certificates.

The continuous publication of the CRLs on the Commerzbank PKI CRL Web servers is performed automatically by the Commerzbank AG Inhouse Sub CA 03; the Commerzbank AG Inhouse Root CA however is published on web servers manually by GS-ITR 4.3 employees, as a network detachment and offline operation is addressed. Commerzbank CA certificates and the CP/CPS Documentation is released by GS-ITR 4.3 and published on the respective Web locations.

Following publication locations are planned:

Commerzbank AG CP/CPS:	http://ca.commerzbank.com/cps/cps.htm
Commerzbank AG CRLs:	http://ca.commerzbank.com/cdp/coba_root.crl
	http://ca.commerzbank.com/cdp/coba_sub03.crl
Commerzbank AG CA certificates:	http://ca.commerzbank.com/aia/coba_root.crt
	http://ca.commerzbank.com/aia/coba_sub03.crt

2.3. Time or frequency of publication

Commerzbank Certificate Policies and the Certification Practice Statement are published after their respective creation resp. revision.

Commerzbank CA certificates are published after installing the Commerzbank CAs. A new publication takes place only after expiration resp. renewal of the CA certificate.

CRLs are created according prescribed schedules and immediately published via the PKI CRL web services.

CRLs issued by the Root CA:	3 months with 1 month overlap
CRLs issued by the Sub CA 03:	weekly with 7 days overlap

The frequency of publication of the external recipient certificates by the Commerzbank Registration Authority Officer is prescribed as defined process. Process information about the Personen PKI can be retrieved from GS-ITR 4.3.

2.4. Access controls on repositories

Access to Commerzbank CA certificates, CRLs, and the CP/CPS documentation is not limited and hence public. See publication locations in chapter 2.2. publication of certification information.

3. Identification and authentication

3.1. Naming

3.1.1. Types of Names

The X.500 Distinguished Name in the CA certificates for Commerzbank subscribers is specified as described in the following tables. The use of DNs for naming in the Subject Name Field allows a one-to-one naming of CAs within the Commerzbank AG.

The naming scheme is identical for all certificates issued by the Commerzbank AG Inhouse Root CA and is created according to the following rules:

CN = [Common Name],
O = [Organization],
L = [Locality],
C = [Country]

In the practical implementation of the PKI not all (naming) attributes are determined, as the significance and clearness of names for the CAs with the necessary attributes is considered sufficient.

3.1.1.1. Commerzbank AG Inhouse Root CA DN

The X.500 Distinguished Name of the self-signed Commerzbank AG Inhouse Root CA reads:

Attribute	Value
E-Mail	***
Common Name (CN)	Commerzbank AG Inhouse Root CA
Organization Unit	***
Organization	Commerzbank AG
Locality	Frankfurt am Main
State or Province	***
Country	DE

3.1.1.2. Commerzbank AG Inhouse Sub CA 03 DN

The X.500 Distinguished Name in the certificate of the Commerzbank AG Inhouse Sub CA 03, which is issued by the Commerzbank Inhouse Root CA, reads:

Attribute	Value
E-Mail	***
Common Name (CN)	Commerzbank AG Inhouse Sub CA 03
Organization Unit	***
Organization	Commerzbank AG
Locality	Frankfurt am Main
State or Province	***
Country	DE

The naming scheme is identical for all certificates issued by the Commerzbank AG Inhouse Sub CA 03 and is created according to the following rules:

E = [RFC 822 eMail Address, optional],
CN = [Common Name],
OU = [Organizational Unit, optional],
O = [Organization],
L = [Locality],
C = [Country]

3.1.1.3. Commerzbank AG smart card certificate DN

The X.500 Distinguished Name in the certificate of end entities **Coba SC Authentication**, which is issued by the Commerzbank Inhouse Sub CA 03, reads:

Attribute	Value
E-Mail	***
Common Name (CN)	Common Name des Commerzbank Benutzers
Organization Unit	***
Organization	Commerzbank AG
Locality	Frankfurt am Main

State or Province	***
Country	DE

The Commerzbank smart card certificate for authentication is used only within the Commerzbank infrastructure and not published outside.

The X.500 Distinguished Name in the certificate of end entities **Coba SC Encryption**, which is issued by the Commerzbank Inhouse Sub CA 03, reads:

Attribute	**Value**
E-Mail	e-mail Adresse des Commerzbank Benutzers
Common Name (CN)	Anzeigename des Commerzbank Benutzers
Organization Unit	***
Organization	Commerzbank AG
Locality	Frankfurt am Main
State or Province	***
Country	DE

The X.500 Distinguished Name in the certificate of end entities **Coba SC Signature**, which is issued by the Commerzbank Inhouse Sub CA 03, reads:

Attribute	**Value**
E-Mail	e-mail Adresse des Commerzbank Benutzers
Common Name (CN)	Anzeigename des Commerzbank Benutzers
Organization Unit	***
Organization	Commerzbank AG
Locality	Frankfurt am Main
State or Province	***
Country	DE

3.1.1.4. Commerzbank AG Zertifikate für Gruppenpostfächer DN

The X.500 Distinguished Name in the certificate of end entities **Commerzbank Soft PSE Encryption**, which is issued by the Commerzbank Inhouse Sub CA 03, reads:

Attribute	Value
E-Mail	e-mail Adresse des Gruppenpostfachs
Common Name (CN)	Name des Gruppenpostfachs
Organization Unit	Team Mailbox
Organization	Commerzbank AG
Locality	Frankfurt am Main
State or Province	***
Country	DE

3.1.2. Need for names to be meaningful

The Distinguished Name has to identify the subscriber unambiguously. If the DN is not sufficient, the unambiguousness of the name can be ensured using the Subject Alternative Name. The following rules apply for naming:

- Certificates may be issued only to a valid name of the subscriber.
  - For authentication certificates for users this is the Common Name of the user and the UPN (User Principle Name) in the Subject Alternative Name Field of the subscriber.
  - For encryption and signature certificates for users this is surname, first name in Common Name and the e-mail address in the Subject Alternative Name Field of the subscriber.
  - For encryption certificates for group mail boxes this is the group mail box name in Common Name and the e-mail address of the group mail box in the Subject Alternative Name Field.
- The DN of the Commerzbank CAs is composed of the name objects Common Name, Organization, Locality, and Country. The unambiguousness of the DN must be ensured with these available name objects.
- The DN of the authentication certificates is composed of the name objects Common Name, Organization, Locality, and Country gebildet. The unambiguousness of the DN must be ensured with these available name objects.
- The DN of the encryption and signature certificates is composed of the name objects Common Name, Organization, Locality, Country, and the Commerzbank user's e-mail address. The unambiguousness of the DN must be ensured with these available name objects.

- The DN of the encryption certificates for group mail boxes is composed of the name objects Common Name, Organization Unit, Organization, Locality, Country, and the group mail boxe's e-mail address. The unambiguousness of the DN must be ensured with these available name objects.
- The alternative name in the encryption and signature certificates contain the holder's e-mail address in the format firstname.surname@commerzbank.com.
- Each certificate is assigned a unique serial number that allows an unambiguous and invariant correlation to the subscriber.

3.1.3. Anonymity or pseudonymity of subscribers

Except technical accounts (service certificates for the management system) or group mail boxes, natural persons as subscribers are not anonymous, neither are pseudonyms used to identify subscribers. Each subscriber (person) can hence be correlated with all assigned certificates.

3.1.4. Rules for interpreting various name forms

The shown Distinguished Names in the certificate profile follow the X.500 standard.
The Commerzbank e-mail addresses and UPN entries in the certificate profile follow the rules of RFC 822. UPN naming information must be available in UTF-8 encoding.

3.1.5. Uniqueness of names

The complete Distinguished Name in certifificates issued by Commerzbank allows unique Names for the Commerzbank CAs as well as for the Commerzbank subscribers.

An additional ID in the Alternative Name Field, namely the unique Commerzbank e-mail address, user UPN information and a unique serial number in the certificates account for this aspect.

3.1.6. Recognition, authentication, and role of trademarks

Usually the DN is limited to natural persons and therefore is irrelevant in accepting trademarks. In general, subscribers and, due to the automated issuance of end-entity certificates, operators of CAs shall ensure the protection of trademarks.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

The key pairs of the commerzbank subscribers are generated on the requesting device in case of group mail box certificates resp. on smart cards for user certificates. The proof of ownership for the private key is performed by signing the PKCS#10 certificate request with the private key. The Certificate Signing Request (CSR) is fundamental for the examination of private keys.

The key pairs of the Commerzbank CAs are generated by the Hardware Security Module. The proof of ownership for the private keys of the CA certificates is performed by signing the PKCS#10 certificate request with the private key. The Certificate Signing Request (CSR) is fundamental for the examination of private keys.

3.2.2. Authentication of organization identity

Not applicable. Only individual certificates for Commerzbank employees or Commerzbank group mail boxes are issued. A certification of employees of other organizations is not performed. External staff with long-term occupations at Commerzbank can apply for a temporary smart card.

3.2.3. Authentication of individual identity

On initial certificate issuance for users and group mail boxes, the RA examines the identity. At thins, necessary steps are taken to unambiguously identify the applicant. Detailled procedures for identification can be learned from the smart card issuance processes description.

3.2.4. Non-verified subscriber information

Only information required to authenticate and identify the subscriber are examined. Other information of the subscriber are not incorporated.

3.2.5. Validation of authority

On issuance of user certificates and group mail box certificates, the authority to apply is verified. Detailled procedures for authority verification can be learned from the smart card issuance processes description.

3.2.6. Criteria for interoperation and cross-certification

Not applicable. At the time of edition, no cross-certification with other organizations is planned.

3.3. Identification and authentication for re-key requests

Identification and authentication on routine certificate renewals with key rotation (e.g. when issuing a new certificate with a new key shortly prior expiration of the old certificate) a successful logon with the personal Windows ID and a one-time-password is sufficient for Commerzbank users and group mail boxes.

3.3.1. Identification and authentication for routine re-key

Renewal of smart card and group mail box certificates is performed automatically by the Personen PKI and the corresponding management system. Concerned certificate users are informed about the pending renewal. For renewal, an authentication against the certificate management system using the Windows ID and a one-time-password is required.

3.3.2. Identification and authentication for re-key after revocation

Identification and authentication for certificate renewal after revocation corresponds to identification and authentication for initial registration.

3.4. Identification and authentication for revocation request

An application system exists. The respective processes for identification and authentication for revocation are prescribed and documented in the application system. In general, subscribers and their superiors can revoke certificates. Detailled information about the application system can be retrieved from GS-ITR 4.3 if necessary.

4. Certificate life-cycle operational requirements

The following chapter lists the general parameters of the Commerzbank Personen PKI. The purpose of the Personen PKI is issuance and management of user and group mail box certificates.

Certificate application for Commerzbank smart card user certificates:

Initial application and renewal of smart card certificates for Commerzbank users is performed controlled by a certificate and smart card management tool. User related certificates are provisioned on a smart card. For this, the certificate life cycle management and the smart card management rests with the management system.

Certificate application for Commerzbank group mail boxes:

Initial application and renewal of smart card certificates for Commerzbank users is performed controlled by a certificate and smart card management tool. For this, the certificate life cycle management and the smart card management rests with the management system.

Use of Commerzbank smart card user certificates:

Authorized uses of Commerzbank smart card certificates include authentication, encryption, and digital signature.

Detailled use cases can be retrieved from the Commerzbank certificate profiles.

Following basic technical conditions are important:

- User certificates are stored on a smart card
- Management and issuance of Commerzbank smart card user certificates is conrolled by the central certificate management tool
- Related CPS, CRL, and CA certificates are published. This facilitates communication.
- S/MIME e-mail certificates are published in the Commerzbank directory service.
- Key archival of encryption keys is established.

Further information about the scope of application of the Personen PKI can be retrieved from GS-ITR 4.3, if necessary.

Use of Commerzbank group mail box certificates:

This certificate is mainly used to encrypt e-mails for group mail boxes. Further uses are excluded.

Following basic technical conditions are important:

- Group mail box certificates exist only as software certificates (Soft PSE).
- Management and issuance of Commerzbank group mail box certificates is conrolled by the central certificate management tool
- Related CPS, CRL, and CA certificates are published. This facilitates communication.
- Group mail box certificates are published in the Commerzbank directory service.
- Key archival of encryption keys for group mail boxes is established.

Further information about the scope of application of the Personen PKI can be retrieved from GS-ITR 4.3, if necessary.

4.1. Certificate application

In the last chapter, chapter 4., the application process is described. Further information about the certificate application can be retrieved from GS-ITR 4.3, if necessary.

4.1.1. Who can submit a certificate application

A certificate application can be submitted by:

- all Commerzbank employees,
- external staff with long-term occupations at Commerzbank. In this case, a temporary smart card is issued.

4.1.2. Enrollment process and responsibilities

Smart cards and group mail box certificates are issued by the Commerzbank Personen PKI. The responsibility for the enrollment process lies with GS-ITR 4.3. A detailed description of the enrollment process and its technical implementation can be retrieved from GS-ITR 4.3, if necessary.

4.2. Certificate application processing

Like certificate application, application processing for smart card and group mail box certificates is controlled by the certificate management system. Detailed information about application processing can be retrieved from GS-ITR 4.3, if necessary.

4.2.1. Performing identification and authentication functions

Applicant identification and authentication is based on valid Commerzbank domain accounts. This applies for smart card applications as well as for applications for Commerzbank group mail box certificates.

4.2.2. Approval or rejection of certificate applications

Applicant approval or rejection is based on valid Commerzbank domain accounts. This applies for smart card applications as well as for applications for Commerzbank group mail box certificates.

4.2.3. Time to process certificate applications

Application processing for smart card and group mail box certificates is controlled by the certificate management system. This procedure allows for immediate certificate issuance to the applicant.

In both use cases, immediate processing takes place. Upstream processes are not considered; they can lead to a longer overall processing time.

4.3. Certificate issuance

Like certificate application, issuance of smart card and group mail box certificates is controlled by the certificate management system.

Further information about certificate issuance can be requested. Detailled procedures for user certificate issuance can be learned from the smart card issuance processes description.

4.3.1. CA actions during certificate issuance

Prior to certificate issuance to the subscribers, the CA performs the following steps:

- Validation of certificate request with the CA policy module
    - In case of controlled issuance by the certificate management system, the validation is performed by the certificate management policy module.
- Achrival of issued certificates and certificate application in the database of the Commerzbank AG Inhouse Sub CA 03.
- Archival of issued certificate information and the application process in the database of the certificate management system. Furthermore, smart card relevant information, like the PUK (admin key) and additional information are stored encrypted in this database.
- When using user encryption keys, these keys are archived in the data base of the Commerzbank AG Inhouse Sub CA 03.
- Certificate issuance for the applicant is performed controlled by the certificate management system.

4.3.2. Notification to subscriber by the CA of issuance of certificate

A notification is performed by the issuing CA and additionally by the Commerzbank Trustcenter.

4.4. Certificate acceptance

Like certificate application, certificate acceptance for user and group mail box certificates certificates is controlled by the Commerzbank certificate management system.

Detailled procedures for certificate acceptance can be learned from the smart card issuance processes description or requested from GS-ITR 4.3.

4.4.1. Conduct constituting certificate acceptance

Certificate acceptance is performed like the application by the Personen PKI.

- For group mail box certificates: As soon as the certificate management system marks the issuance as “completed”.
- For user certificates: As soon as the certificate management system marks the issuance as “completed”.

4.4.2. Publication of the certificate by the CA

The encryption certificate is automatically published by the Personen PKI in the local directory service. No user interverntion is necessary.

The Commerzbank CA certificates for Commerzbank AG Inhouse Root CA and Commerzbank AG Inhouse Sub CA 03 is published on the PKI web servers manually by GS-ITR 4.3. This also appies for renewal of the above CA certificates.

4.4.3. Notification of certificate issuance by the CA to other entities

There is no notification of issuance to other entities by the Commerzbank CAs.

4.5. Key pair and certificate usage

Generally, the key pair is provided for authentication, for en- and decryption of information, and for creation/validation of signatures.

4.5.1. Subscriber private key and certificate usage

The subscriber has to use the certificates according to the Commerzbank certificate policies. Chapter 1.4. certificate usage lists authorized and prohibited uses of keys and certificates. Furthermore, the subscriber has to fulfil his duties according Commerzbank smart card policy when using his private keys.

4.5.2. Relying party public key and certificate usage

Relying parties have to use the certificates according to their organizations' applicable certificate policies. Those list authorized and prohibited uses of keys and certificates.

4.6. Certificate renewal

In the scope of the Commerzbank Personen PKI certificate renewal is always connected with key change. Certificate life cycle renewal while maintaining key pairs is not allowed for. Therefore, the following subchapters in 4.6. are not applicable for the Commerzbank Personen PKI.

4.6.1. Circumstance for certificate renewal

Not applicable.

4.6.2. Who may request renewal

Not applicable.

4.6.3. Processing certificate renewal requests

Not applicable.

4.6.4. Notification of new certificate issuance to subscriber

Not applicable.

4.6.5. Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6. Publication of the renewal certificate by the CA

Not applicable.

4.6.7. Notification of certificate issuance by the CA to other entities

Not applicable.

4.7. Certificate re-key

In the scope of the Commerzbank Personen PKI certificate renewal is always connected with key change. A modification of certificate contens (data modification, certificate modification) is planned for, as personal data like e-mail address and name may change over a life cycle. All following subchapters in 4.7. are not applicable for the Commerzbank Personen PKI.

4.7.1. Circumstance for certificate re-key

Not applicable.

4.7.2. Who may request certification of a new public key

Not applicable.

4.7.3. Processing certificate re-keying requests

Not applicable.

4.7.4. Notification of new certificate issuance to subscriber

Not applicable.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6. Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7. Notification of certificate issuance by the CA to other entities

Not applicable.

4.8. Certificate modification

In the scope of the Commerzbank Personen PKI certificate renewal is always connected with key change. Technically, the old certificate is replaced by a certificate with new validity time and new public key (and new private key) and possible modification of content data.

4.8.1. Circumstance for certificate modification

Certificate modification can be requested if following circumstances apply:

- the old certificate's life span is expired or is about to expire
- the old certificate was revoked

- the old certificate's content data are incorrect
- the old key cannot be used any longer, because of a (possible) compromise
- the old certificate's life span or the old key's length do not provide sufficient security any more
- technical unsuability (loss of private key or loss of access to private key)

4.8.2. Who may request certificate modification

All subscribers, who have been assigned a valid certificate by the Personen PKI and who are:

- Commerzbank employees,
- external staff with long-term occupations at Commerzbank. Temporary smart cards are issued to external staff.

4.8.3. Processing certificate modification requests

The process is similar to the initial application. The Commerzbank Personen PKI processes the certificate modification for smart card user certificates and group mail box certificates controlled by the certificate and smart card management system.

4.8.4. Notification of new certificate issuance to subscriber

During controlled certificate issuance and modification by the certificate and smart card management system, a renewal notification is sent to the applicant via e-mail. The renewal notification is sent to the participants during the renewal interval

4.8.5. Conduct constituting acceptance of modified certificate

Certificate acceptance is performed like the application by the Personen PKI.

- For group mail box certificates: As soon as the certificate management system marks the issuance as "completed".
- For user certificates: As soon as the certificate management system marks the issuance as "completed".

4.8.6. Publication of the modified certificate by the CA

The encryption certificate is automatically published by the Personen PKI in the local directory service. No user interverntion is necessary.

The Commerzbank CA certificates for Commerzbank AG Inhouse Root CA and Commerzbank AG Inhouse Sub CA 03 is published on the PKI web servers manually by GS-ITR 4.3.

4.8.7. Notification of certificate issuance by the CA to other entities

There is no notification of issuance to other entities by the Commerzbank CAs.

4.9. Certificate revocation and suspension

Primarily, a certificate revocation is planned, not a certificate suspension. Further information about certificate revocation can be retrieved from GS-ITR 4.3.

4.9.1. Circumstances for revocation

A certificate has to be revoked:

- If the Commerzbank user smart card has been stolen, damaged or lost, i.e. as soon as a permanent replacement smart card with new certificates is issued.
- If a reasonable suspicion exists, that the private key corresponding to the public key of the certificate was compromised, i.e. that an unauthorized person can use the private key.
- If a reasonable suspicion exists, that the algorithms, parameters, and devices used for the generation and application of the private key corresponding to the public key of the certificate no longer garant protection against forgery.
- If the subscriber can no longer use his certificate, e.g. if the user cannot access his encryption keys any more.
- If a certificate modification or renewal was requested or will be requested soon.
- If the Commerzbank AG discontinues its certificate services. In this case, all certificates are revoked that were issued by the certificate services.
- If the subscriber does not fulfil the certificate application requirements any more, e.g. because a Commerzbank employee discontinues his employment or he violates the current certificate policy.

4.9.2. Who can request revocation

Following groups of persons and instances can request certificate revocation:

- Revocation of a certificate can be requested by
    - the subscriber,
    - his representative (by warrant),
    - his superiror.
- Revocation of a CA certificate can be requested by a Commerzban RA Officer.

4.9.3. Procedure for revocation request

A certificate revocation takes place via e-mail or telephone. The person requesting revocation is identified with appropriate means.

A certificate revocation is generally performed by the Commerzbank RA Officer or the LRO using the certificate and smart card management system of the Commerzbank Personen PKI.

4.9.4. Revocation request grace period

No grace periods are prescribed. Generally, a notification about a revocation request should take place as soon as possible.

4.9.5. Time within which CA must process the revocation request

No time is prescribed within wich CA must process the revocation request.

4.9.6. Revocation checking requirement for relying parties

A revocation checking is recommended for relying parties. The revocation status of Commerzbank certificates and Commerzbank CA certificates can be checked via the corresponding CRLs. Current CRLs can be downloaded from the CDPs (CRL Distribution Points) contained in the certificate.

4.9.7. CRL issuance frequency

Following issuance schemes apply for the Commerzbank Personen PKI:

Commerzbank Inhouse Root CA:

- CRL issuance frequency: 3 monts
- CRL issuance overlap: 1 month

Commerzbank Inhouse Sub CA 03:

- CRL issuance frequency: 1 week
- CRL issuance overlap: 1 week

4.9.8. Maximum latency for CRLs

- CRLs are available on the Commerzbank PKI web servers immediately after issuance. No latency must be expected for CRLs.

4.9.9. On-line revocation/status checking availability

Not applicable. Online revocation and status checking are not planned for the Commerzbank Personen PKI.

4.9.10. On-line revocation checking requirements

Not applicable.

4.9.11. Other forms of revocation advertisements available

No further. Commerzbank CRLs are published on web server locations which are published via the CDP entries in the certificate.

4.9.12. Special requirements in case of private key compromise

If there is a cue for a key compromise, an investigation is performed. If the compromise can be proven, necessary steps are taken, like revocation of concerned certificates.

4.9.13. Circumstances for suspension

Not applicable; a complete revocation is planned for the certificate.

4.9.14. Who can request suspension

Not applicable; a complete revocation is planned for the certificate.

4.9.15. Procedure for suspension request

Not applicable; a complete revocation is planned for the certificate.

4.9.16. Limits on suspension period

Not applicable; a complete revocation is planned for the certificate.

4.10. Certificate status services

The Commerzbank AG operates a certificate status service. This service is web-based and is represented by the URL http://ca.commerzbank.com/cdp/. The CRLs are published:

- Status information about end-entity certificates are published in the CRL issued by the Commerzbank AG Inhouse Sub CA 03.
- Status information about CA certificates are published in the CRL issued by the Commerzbank AG Inhouse Root CA.

For each certificate type, an own CRL is published.

4.10.1. Operational characteristics

The status service is web-based and uses HTTP as transport protocol.

The CRLs of Root CA and Sub CA 03 can be retrieved from following URLs:

- http://ca.commerzbank.com/cdp/coba_root.crl
- http://ca.commerzbank.com/cdp/coba_sub03.crl

CRL and certificate to be revoked have to be issued by the same CA. The current implementation does not support “indirect CRLs”.

The issued CRL profile complies with RFC 5280 and the X.509 Version 2 standard.

4.10.2. Service availability

The Commerzbank PKI web server is designed for 24/7 operation.

4.10.3. Optional features

None.

4.11. End of subscription

A Commerzbank certificate subscription ends, when the subscriber’s employment at Commerzbank AG ends. This includes external staff.

4.12. Key escrow and recovery

The Commerzbank Personen PKI implements key escrow and recovery for encryption keys.

Recovery of user keys is performed using a backup copy of the keys. This is implemented by the smart card management system and the related CA Commerzbank AG Inhouse Sub CA 03, which stores the users encryption keys in the CA database in encrypted form. A detailed process description can be requested from GS-ITR 4.3.

4.12.1. Key escrow and recovery policy and practices

In the Scope of the Commerzbank Personen PKI a key recovery policy has been established. A detailed process description can be requested from GS-ITR 4.3.

In Rahmen der Commerzbank Personen PKI wurde eine Wiederherstellungsrichtlinie erarbeitet. Eine Detailbeschreibung dieses Prozesses kann von der GS-ITR 4.3 erfragt werden.

4.12.2. Session key encapsulation and recovery policy and practices

Not applicable. Session keys are not archived.

5. Facility, management, and operational controls

5.1. Physical controls

The Commerzbank Personen PKI infrastructure controls are embedded in the Commerzbank AG data center operation. Following provisions and physical controls are integral part of the Commerzbank AG data centers.

5.1.1. Site location and construction

The Commerzbank Personen PKI systems reside in the Commerzbank data center premises. The premises offer sufficient physical controls for the appropriate security level.

5.1.2. Physical access

The CA operating rooms are secured by appropriate technical and infrastructural controls. Access to CA operating rooms is granted only to employees with the required security clearance. Access for external persons is defined by a visitor policy.

5.1.3. Power and air conditioning

Power installation fulfils the relevant standards, air conditioning is provided for technical infrastructure premises.

5.1.4. Water exposures

The technical infrastructure premises are adequately protected against water exposures.

5.1.5. Fire prevention and protection

Applicable fire protection requirements are fulfilled.

5.1.6. Media storage

Following media is used:

- Paper
- CD-ROMs
- USB storage modules
- Tapes
- Hardware tokens

Media is stored in closed lockers. Media with sensitive data, like HSM hardware tokens, is stored in a safe.

5.1.7. Waste disposal

Information on electronic media is correctly wiped and afterwards disposed of properly. Paper media is destroyed with on-site document shredders and afterwards disposed of properly.

5.1.8. Off-site Backup

The Commerzbank data center operation cares for off-site backups.

5.2. Procedural controls

5.2.1. Trusted Roles

Security relevant tasks for operation of the Commerzbank Personen PKI are combined in roles. A PKI role concept is available and is used for organizational processes and HSM operation.

A role definition description can be requested from GS-ITR 4.3, if necessary.

5.2.2. Number of persons required per task

Following tasks require four-eye-principle:

- Key recovery for Commerzbank CAs
- Recovery of Commerzbank CAs
- Access to Commerzbank CA HSMs

5.2.3. Identification and authentication for each role

Identification and authentication of users is required prior to entering security relevant premises and when accessing security relevant systems using smart cards, hardware tokens, and/or username and password.

For particular security relevant operations, like management of CA keys, a four-eye-principle is applied.

5.2.4. Roles requiring separation of duties

The role concept also defines, which role assignments do mutually exclude each other. Detailled information about role and duty separation can be requested from GS-ITR 4.3.

5.3. Personnel controls

Commerzbank AG provides experienced personnel for the Personen PKI. Required qualification, knowledge, and experience for a secure PKI operation are available.

5.3.1. Qualifications, experience, and clearance requirements

The responsible personnel has specific knowledge and experience in the area of the Personen PKI. Furthermore, general IT knowledge is available to perform system-related operations.

5.3.2. Background check procedures

The general employment policies of the Commerzbank AG apply.

5.3.3. Training requirements

Personnel employed in the certification service is sufficiently trained prior to operational employment. The training encompasses an awareness training for the security relevance of their task and potential threats.

5.3.4. Retraining frequency and requirements

The retraining frequency is adapted to the Commerzbank Personen PKI's requirements. Trainings are primarily performed on introduction of new policies, IT systems, and security technologies.

5.3.5. Job rotation frequency and sequence

Job rotation is not planned.

5.3.6. Sanctions for unauthorized actions

General sactions of Commerzbank AG are applied in case of unauthorized actions.

5.3.7. Independent contractor requirements

The Commerzbank PKI operations personnel commits to adherence to directives and legal provisions. These include the obligation to keep personal data confidential.

5.3.8. Documentation supplied to personnel

Following documentation is supplied to Commerzbank personal for proper operation of the Personen PKI:

- Certificate Policy (CP)
- Certification Practice Statement (CPS)
- Operations and security concept for Personen PKIs
- Directives
- Operations manuals of systems and software

5.4. Audit logging procedures

5.4.1. Types of events recorded

For each event, following data is recorded:

- Timestamp (date and time of day)
- Log ID of entry
- Type of event
- Origin of Ereignisses

5.4.2. Frequency of processing log

A processing of log data should be performed regularly. If there is any suspect of irregularities, an immediate processing is performed.

5.4.3. Retention period for audit log

Audit log files are stored according to legal regulations.

5.4.4. Protection of audit log

Electronic log files are protected against access, deletion, and manipulation with operating system tools. They are accessible only to system and network administrators.

5.4.5. Audit log backup procedures

Audit logs are backed up regularly together with other data. Audit logs on paper media are stored in lockable cabinets.

5.4.6. Audit collection system (internal vs. external)

All audit log files are regularly backed up.

5.4.7. Notification to event-causing subject

The PKI personnel is notified if an operational distruption occurs.

5.4.8. Vulnerability assessments

Not applicable.

5.5. Records archival

The Commerzbank AG archives the necessary records connected with operation of the Personen PKI.

5.5.1. Types of records archived

Data, which is important for the certification process, is archived:

- Certificate applications, they contain personal data of the applicant
- All certificates issued by the CA
- Revocation requests for certificates and CA certificates
- System data saved prior modifications
- Productive system backups
- Documentation of personnel controls (e.g. duty rosters, security check documentation)
- Documentation of procedures and systems (e.g. directives, emergency plans, sytem manuals)
- Records of security relevant internal processes and procedures

5.5.2. Retention period for archive

Archives are retained according to Commerzbank regulations.

5.5.3. Protection of archive

Appropriate means ensure that data cannot be altered or deleted. If personal data is contained in the archives, the data is additionally protected against unauthorized access or copying.

Protective measures for electronic media comply with the processes for Commerzbank AG data center operation.

5.5.4. Archive backup procedures

Procedures and processes for archive backup comply with the implementation for Commerzbank AG data center operation.

5.5.5. Requirements for time-stamping of records

Audit logs, recorded events, archived data, certificates, CRLs, and other entries obtain an unambiguous time and date information. Date and time information of online systems are regularly synchronized with a trusted time source.

5.5.6. Archive collection system (internal or external)

An archive collection system is used in conjunction wit the Commerzbank Personen PKI.

5.5.7. Procedures to obtain and verify archive information

The Commerzbank AG Personen PKI operational concept describes processes for application and verification of archive information. A detailed process description can be restquested from GS-ITR 4.3.

5.6. Key changeover

In case of key changeover of the Commerzbank AG Inhouse Root CA, the old CA certificate is destroyed and a new, self-signed certificate is issued and published. Revocation of the self-signed Root CA certificate is technically impossible.

In case of key changeover of the Commerzbank AG Inhouse Sub CA 03 for user certificates, the Inhouse Sub CA 03 certificate is revoked by the Commerzbank AG Inhouse Root CA and a new certificate is issued and published. Application is performed by the Commerzbank AG Inhouse Sub CA 03.

CA key changeover follows the below scheme:

Commerzbank AG Inhouse Root CA

- Root CA certificate: 30 years
- Root CA CRLs: 4 months
- Renewal of Commerzbank AG Inhouse Root CA certificate latest 12 months prior expiration

Commerzbank AG Inhouse Sub CA 03

- Sub CA 03 certificate: 10 years
- Sub CA 03 CRLs: 12 days
- Renewal of Commerzbank AG Inhouse Sub CA 03 certificate latest 6 months prior expiration

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

Commerzbank AG has disaster recovery plans that define processes, procedures, and responsibilities in case of disasters. The disaster recovery plans' aim is minimal downtime of certificate services while maintaining security. Contingency procedures particularly envies following tasks in case of incidents:

- Analysis and evaluation of functional degrade and security problems of affected CA systems and services.
- Definition of immediate response actions to counteract functional degradations and security issues.
- Settlement of roles and responsibilities.
- Notification of affected persons and instances, if necessary, e.g. subscribers, about the issue and necessary actions.
- Causes analysis and documentation.
- Creation, evaluation, and approval of a change request, if appropriate, to modify the system configuration to prevent issues of this type. Monitoring of change request implementation.
- Logging of tasks and actions.

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

If faulty or manipulated computers, software, and/or data is detected within the CA, which affect CA processes,

- operation of the affected IT system is immediately ceased,
- the affected IT system is reinstalled, recovering software and data from backups, checked, and brought to secure operation.
- Following, the faulty or modified IT system is evaluated. If there is any suspect of a deliberate compromise, legal steps are taken.
- If a certificate contains wrong data, the subscriber is immediately informed and the certificate is revoked.

5.7.3. Entity private key compromise procedures

Compromise of private keys is a serious issue and therefore specially handeled.

- If private keys of a CA certificate are compromised, the respective certificate is immediately revoked. At the same time, all certificates issued with the compromised certificate are also revoked.

- If private keys of a Commerzbank smart card user certificate or group mail box certificate are compromised, the respective certificate is immediately revoked.
- If there is any suspect that the algorithms, parameters, or devices used for creation and application of private keys are insecure, an investigation is performed.
- All affected subscribers and relying parties are informed immediately.

5.7.4. Business continuity capabilities after a disaster

Recovery of certificate services operation after a disaster is part of contingency/disaster planning and can be accomplished in short time, if safety of certificate services is assured.

5.7.5. CA or RA termination

In case of Commerzbank CA or RA termination, following tasks are defined:

- All subscribers and relying parties are informed about certificate services termination. No time limit is prescribed.
- All CA and user certificates are revoked.
- All private keys of CA and subscriber smart card certificates are destroyed.
- Encryption keys are exempted. They are stored in secure environments, like an encrypted database.

6. Technical security controls

6.1. Key pair generation and installation

6.1.1. Key pair generation

Key generation and selection of encryption algorithms for Commerzbank Personen PKI is performed according FIPS 140-2 Level 1 resp. 3 (Federal Information Processing Standards).

Key pair generation is performed by hard- and software components and depends on the entity:

Key pair generation for Commerzbank CAs:

All key pairs for Commerzbank CAs are generated by the Network HSM (Hardware Security Module). The generated CA keys are cryptographically secured by the HSM. Each process that requires access to the CA's private key mandatorily involves the HSM. The Commerzbank Network HSM is operated in FIPS 140-2 Level 3 mode.

Key pair generation for Commerzbank group mail box certificates:

Key pairs for Commerzbank group mail boxes are generated by the Personen PKI on behalf of Commerzbank subscribers. Generation of keys is performed by software components. The cryptographic software components are certified according FIPS 140-2 Level 1.

Key pair generation for Commerzbank smart card user certificates:

Authentication and signature key pair for smart card user certificates are generate by the smart card for Commerzbank subscribers. In this case, the keys are generated by hardware. The smart card's cryptographic hardware components are certified according FIPS 140-2 Level 3.

On the other hand, the encryption key pair is generated by cryptographic software components. This allow archival of encryption keys. The cryptographic software components are certified according FIPS 140-2 Level 1.

6.1.2. Private key delivery to subscriber

Commerzbank CAs' private keys:

Each process that requires access to the CA's private key mandatorily involves the HSM; all private CA keys reside in the HSM only.

Delivery is not necessary for CA private keys, as the HSM accomplishes both generation and secure storage of private keys. Backup tokens are used as storage for private key material on the HSM.

Smart card user certificate private keys:

The smart card is delivered to the Commerzbank subscriber. Initially, the smart card contains no key pairs or certificates. During provisioning, key pairs for user certificates are generated on the used smart card or, in case of encryption keys, stored on the smart card later.

Access to private keys is possible only after authentication with user PIN.

Commerzbank group mail box certificate private keys:

Key pairs are generated on the requesting machines.

A following manual delivery is not necessary. In this case, the private key is delivered automatically to the requesting machine via appropriate secure means, like PKCS#12.

6.1.3. Public key delivery to certificate issuer

The Certificate Signing Request (CSR) of the subscriber is transmitted to the CA in PKCS#10 format by the Personen PKI for certification. The process takes place automatically.

The Commerzbank AG Inhouse Sub CA 03 Certificate Signing Request is also transmitted in PKCS#10 format. However, this process is carried out manually due to the offline characteristic of the Commerzbank AG Inhouse Root CA.

6.1.4. CA public key delivery to relying parties

CA public key delivery is performend manually. Furthermore, Commerzbank CA public keys are available on the prescribed web URLs:

Commerzbank AG Inhouse Root CA: http://ca.commerzbank.com/aia/coba_root.crt

Commerzbank AG Inhouse Sub CA 03: http://ca.commerzbank.com/aia/coba_sub03.crt

6.1.5. Key sizes

Commerzbank CA key size:

- Commerzbank AG Inhouse Root CA – 4096bit (HSM) – RSA algorithm
- Commerzbank AG Inhouse Sub CA 03 – 2048bit (HSM) – RSA algorithm

Commerzbank subscriber key size:

- Commerzbank smart card user certificates – 2048bit – RSA algorithm
- Commerzbank group mail box certificates – 2048bit – RSA algorithm

6.1.6. Public key parameters generation and quality checking

- Public key algorithm: 1.2.840.113549.1.1.1 (RSA)
- Signature algorithm: 1.2.840.113549.1.1.5 (sha1RSA)

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

See also chapter 7.1 certificate and CRL profilee.

Commerzbank CA key usage:

- Commerzbank AG Inhouse Root CA – digital signature, certificate signing, certificate trust list signing, certificate trust list signing (offline)
- Commerzbank AG Inhouse Sub CA 03 – digital signature, certificate signing, certificate trust list signing, certificate trust list signing (offline)

Commerzbank subscriber key usage:

- Commerzbank group mail boxes – key encipherment
- Commerzbank smart card (authentication) – digital signature
- Commerzbank smart card (encryption) – key encipherment
- Commerzbank smart card (signature) – digital signature, non-repudiation

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Private keys in the Commerzbank Personen PKI are protected by cryptographic hardware or software modules.

Private keys of Commerzbank CAs are protected by a Hardware Security Module, Commerzbank subscriber private keys are protected by software and hardware implementations of the cryptographic interface.

Protection of private keys of

- Commerzbank CAs is accomplished by the Hardware Security Module.
- Commerzbank smart card certificates is accomplished by a hardware implementation of the cryptographic interface on the smart card.
- Commerzbank group mail box certificates is accomplished by a software implementation of the cryptographic interface.

6.2.1. Cryptographic module standards and controls

- The deployed Network HSM is evaluated according FIPS 140-2, Level 2 and Level 3.
- Deployed smart cards are evaluated according FIPS 140-2, Level 3.
- Deployed cryptographic software modules are evaluated according FIPS 140-2, Level 1.

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

There is no splitting of private keys. The Network HSM is exempted. An n-out-of-m-procedure is deployed for the Network HSM management.

6.2.3. Private key escrow

The Commerzbank CAs' private keys are escrowed via HSM Backup Tokens.

6.2.4. Private key backup

The Commerzbank CAs' private keys are backed up by the Network HSM and the related HSM Backup Tokens and processes.

The Commerzbank subscribers' private keys are backed up with the backup mechanisms offered by the Personen PKI. A detailed description of both above processes can be requested from GS-ITR 4.3.

6.2.5. Private key archival

Only private encryption keys are archived. There is a backup/archive for private key revocery. Detailed information can be requested from GS-ITR 4.3.

6.2.6. Private key transfer into or from a cryptographic module

A transfer of private keys is envisaged only for encryption keys. For this, the keys are generated outside the cryptographic module (smart card) and imported into the cryptographic module (smart card) afterwards. This procedure is necessary to archive encryption keys.

The Commerzbank CAs' private keys are backed up by dedicated backup components (backup tokens) and processes of the Network HSM.

6.2.7. Private key storage on cryptographic module

The Commerzbank AG Inhouse Root CA's and Commerzbank AG Inhouse Sub CA 03's private keys are managed and secured by the Network HSM. Furthermorge, the Network HSM backs up the CA keys and stores the backup in a physically secured location. The Network HSM is certified according FIPS 140-2, Level 3.

The smart card user certificates' private keys are secured by the deployed smart card and stored on a protected area on the smart card. The deployed smart cards are certified according FIPS 140-2, Level 3.

The Commerzbank group mail box certificates' private keys are managed and securely stored by a cryptographic software component on the requesting machine. The cryptographic software components are certified according FIPS 140-2, Level 1.

6.2.8. Method of activating private key

Activation of private keys is envisaged only for Commerzbank smart card user keys. Activation and access on private keys is done by setting a smart card PIN by the user.

6.2.9. Method of deactivating private key

Not applicable. A deactivation of private keys is not envisaged for the Commerzbank Personen PKI.

6.2.10. Method of destroying private key

Methods of destroying private keys by the certificate services provider depends on the cryptographic hard- and software which stores the keys:

- Destroying of all private keys is usually perfomed by deleting the private key storage. An individual deletion of private keys has to be performed manually.
- CA's private keys, which are stored in HSMs, can be destroyed by deleting them from the HSM.

- Private keys on smart cards are deleted by initialization resp. formatting.

6.2.11. Cryptographic Module Rating

- The deployed Network HSM is operated according FIPS 140-2, Level 3.
- The deployed smart cards are operated according FIPS 140-2, Level 3.
- The deployed cryptographic software modules are operated according FIPS 140-2, Level 1.

6.3. Other aspects of key pair management

6.3.1. Public key archival

All certificates issued by the certificate servies are archived in the CA database. There is no further archival of public keys.

6.3.2. Certificate operational periods and key pair usage periods

Following life spans are defined for the Commerzbank AG certificate authorities:

Commerzbank AG Inhouse Root CA

- Root CA certificate: 30 years
- Root CA CRLs: 4 months
- Certificate renewal with key change

Commerzbank AG Inhouse Sub CA 03

- Sub CA 03 certificate: 10 years
- Sub CA 03 CRLs: 14 days
- Certificate renewal with key change

Commerzbank AG Zertifikate für Smart Cards

- Commerzbank smart card certificates: 3 years
- Certificate renewal with key change

Commerzbank AG Zertifikate für Gruppenpostfächer

- Commerzbank group mail box certificate: 3 years
- Certificate renewal with key change

6.4. Activation data

In the scope of implementation of the Commerzbank Personen PKI activation data accrue, which control access to private keys. As activation data, on issuance of smart cards, a user PIN and PUK is created for Commerzbank users.

6.4.1. Activation data generation and installation

Random creation of activation data (PUK) is performed by the certificate and smart card management system.

6.4.2. Activation data protection

Activation data (PUK) is protected by the certificate and smart card management system. For this, these data are stored encrypted on the according certificate management database. Access on those is limited exclusively to the certificate management system.

6.4.3. Other aspects of activation data

Not applicable.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

Servers implementing central functions of certificate servies as well as all computers protecting certificate services facilities have to fulfil the following security requirements:

- Only software necessary for the specific functionality is installed on the server.
- The server has only communication interfaces that are required for the specific functionality. This particularly means that these computers are only integrated in the necessary network parts.
- Unnecessary operating system and software functionality is deactivated, if possible.
- If security risks in deployed software become known, system administrators apply countermeasures recommended by the vendor or independent professionals in due time. In particular, the operating system and deployed software is always patched against known vulnerabilities.
- Access to serves is limited to the amont necessary for certificate services operation. In particular, servers are managed only by responsible system administrators.
- Security relevant events on computers are logged.
- Systems with high availability demand are designed highly available, so as to maintain functionality if a computer fails.
- Power supply jitter and power losses up to several hours are bridged with uninterruptible power supplies and power plants.
- Only virus checked media may be used on these systems.

6.5.2. Computer security rating

The Commerzbank Personen PKI is based on certificate servies, which are evaluated according Common Criteria EAL (Evaluation Assurance Level) 4+ (FLR – augmented with Flow Remediation).

The deployed Network HSM is evaluated according FIPS 140-2, Level 2 and Level 3.

The deployed smart cards are evaluated according FIPS 140-2, Level 3.

The deployed cryptographic software modules are evaluated according FIPS 140-2, Level 1.

6.6. Life cycle technical controls

6.6.1. System development controls

Not applicable.

6.6.2. Security management controls

Not applicable.

6.6.3. Life cycle security controls

Within the security concept for the Commerzbank Personen PKI and related CAs, necessary security controls are evaluated. Detailled information about the security concept can be requested from GS-ITR 4.3.

6.7. Network security controls

Certificate services implement following network security controls:

- Productive systems and networks are separated from the Internet with firewalls.
- The certificate services' internal networks are separated according to their respective security demand. Separation is accomplished with firewalls.
- Firewalls limit data traffic to the extend necessary for operation

6.8. Time-stamping

Commerzbank CAs use time stamps on certificate and CRL issuance. The used time source is the used computer's local system clock. The online servers' local system clock is regularly synchronized with an external time source. Time synchronization of the Commerzbank Inhouse Root CA is accomplished manually.

Deployment of a trusted and evaluated time source is not necessary for the Personen PKI solution.

7. Certificate, CRL, and OCSP profiles

Certificate and CRL profiles are defined in the scope of the Personen PKI for the Commerzbank AG Inhouse Root CA. These Profile follow the regulations of PKIX according RFC 5280 and focus on interoperability issues. Extensions for certificate and CRL profiles are planned, as long as they can be used to distinguish between certificate types.

7.1. Certificate profile

Commerzbank certificates comply with:

- ITU-T recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Juni 1997.

Commerzbank certificate profiles comply with:

- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
- RFC 5280 (succeeding RFC 3280): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

Commerzbank certificates' base description contains:

Key	**Value**
Version	See *7.1.1. Version number(s)*
Serial Number	Unique value in the namespace of each CA
Signature Algorithm	Designation of algorithm used to sign the certificate. See *7.1.3. Algorithm object identifiers*
Issuer	See *7.1.4. Name Forms*
Validity	Validity (from and to) time and date information.'
Subject	See *7.1.4. Name Forms*
Subject Public Key	Public Key Blob
Signature	CAs signature

Commerzbank AG CA certificates

Commerzbank AG Inhouse Root CA	
X.509 Version	V3
Serial Number	03 99 01 d4 0f a3 37 b3 49 71 9d 48 f7 52 b7 e8
Signature Algorithm	sha1RSA
Issuer	CN = Commerzbank AG Inhouse Root CA O = Commerzbank AG L = Frankfurt am Main C = DE
Key Length	4096

Valid from	Wednesday, December 7th, 2005 14:15:17
Valid to	Friday, December 7th, 2035 14:16:04
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = Commerzbank AG Inhouse Root CA O = Commerzbank AG L = Frankfurt am Main C = DE
Key Usage	Digital Signature, Certificate Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline)
Subject Key Identifier	8c f9 89 bf 7e 3c ca 24 31 cc 70 c6 95 9d 72 47 36 27 c8 67
Authority Key Identifier	None
CRL Distribution Points	None
Authority Information Access	None
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	9c 36 c6 c6 9e 7d ec 92 5b 7e 1b 88 e5 64 c4 cd a6 87 c4 2c

Commerzbank AG Inhouse Sub CA 03	
X.509 Version	V3
Serial Number	61 07 1e 53 00 00 00 00 00 06
Signature Algorithm	sha1RSA
Issuer	CN = Commerzbank AG Inhouse Root CA O = Commerzbank AG L = Frankfurt am Main C = DE
Key Length	2048
Valid from	Wednesday, June 27th, 2007 11:13:45
Valid to	Tuesday, June 27th, 2017 11:23:45
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = Commerzbank AG Inhouse Sub CA 03 O = Commerzbank AG L = Frankfurt am Main C = DE
Key Usage	Digital Signature, Certificate Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline)
Subject Key Identifier	d5 b6 fa fa 21 9f 06 eb c4 f2 cb f7 36 60 cb 3b 8c f0 3f a0
Authority Key Identifier	8c f9 89 bf 7e 3c ca 24 31 cc 70 c6 95 9d 72 47 36 27 c8 67
CRL Distribution Points	http://ca.commerzbank.com/cdp/coba_root.crl
Authority Information Access	http://ca.commerzbank.com/aia/coba_root.crt

Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	sha1
Thumbprint	11 cd e7 32 6d a3 5e e1 42 fc 99 4f 70 af ad fd c4 c4 6e 66

Commerzbank AG smart card certificates

Coba SC Authentication	
X.509 Version	V3
Serial Number	[Certificate Serial Number]
Signature Algorithm	sha1RSA
Issuer	CN = Commerzbank AG Inhouse Sub CA 03 O = Commerzbank AG L = Frankfurt am Main C = DE
Key Length	2048
Valid from	[Start date and time]
Valid to	[End date and time]
Public Key	RSA (2048-Bit) Key Blob
Subject	CN = <Comsi ID> O = Commerzbank AG L = Frankfurt am Main C = DE
Key Usage	Digital Signature
Subject Key Identifier	[corresponding private key]
Authority Key Identifier	d5 b6 fa fa 21 9f 06 eb c4 f2 cb f7 36 60 cb 3b 8c f0 3f a0
CRL Distribution Points	http://ca.commerzbank.com/cdp/coba_sub03.crl
Authority Information Access	http://ca.commerzbank.com/aia/coba_sub03.crt
Subject Alternative Name	<User Principal Name>
Extended Key Usage	Smart card logon (1.3.6.1.4.1.311.20.2.2) Client authentication (1.3.6.1.5.5.7.3.2)
Thumbprint Algorithm	sha1
Thumbprint	[Thumbprint of certificate]

Coba SC Signature	
X.509 Version	V3
Serial Number	[Certificate Serial Number]

Signature Algorithm	sha1RSA
Issuer	CN = Commerzbank AG Inhouse Sub CA 03 O = Commerzbank AG L = Frankfurt am Main C = DE
Key Length	2048
Valid from	[Start date and time]
Valid to	[End date and time]
Public Key	RSA (2048-Bit) Key Blob
Subject	E = <e-mail address> CN = <surname>, <first name> O = Commerzbank AG L = Frankfurt am Main C = DE
Key Usage	Digital signature, non-repudiation
Subject Key Identifier	[corresponding private key]
Authority Key Identifier	d5 b6 fa fa 21 9f 06 eb c4 f2 cb f7 36 60 cb 3b 8c f0 3f a0
CRL Distribution Points	http://ca.commerzbank.com/cdp/coba_sub03.crl
Authority Information Access	http://ca.commerzbank.com/aia/coba_sub03.crt
Subject Alternative Name	<RFC 822 e-mail address>
Extended Key Usage	Secure e-mail (1.3.6.1.5.5.7.3.4) Document signature (1.3.6.1.4.1.311.10.3.12)
Thumbprint Algorithm	sha1
Thumbprint	[Thumbprint of certificate]

Coba SC Encryption	
X.509 Version	V3
Serial Number	[Certificate Serial Number]
Signature Algorithm	sha1RSA
Issuer	CN = Commerzbank AG Inhouse Sub CA 03 O = Commerzbank AG L = Frankfurt am Main C = DE
Key Length	2048
Valid from	[Start date and time]
Valid to	[End date and time]
Public Key	RSA (2048-Bit) Key Blob
Subject	E = <e-mail address> CN = <surname>, <first name> O = Commerzbank AG L = Frankfurt am Main C = DE

Key Usage	Key Encipherment
Subject Key Identifier	[corresponding private key]
Authority Key Identifier	d5 b6 fa fa 21 9f 06 eb c4 f2 cb f7 36 60 cb 3b 8c f0 3f a0
CRL Distribution Points	http://ca.commerzbank.com/cdp/coba_sub03.crl
Authority Information Access	http://ca.commerzbank.com/aia/coba_sub03.crt
Subject Alternative Name	<RFC 822 eMail address>
Extended Key Usage	BitLocker drive encryption (1.3.6.1.4.1.311.67.1.1) Secure e-mail (1.3.6.1.5.5.7.3.4) Encrypting file system (1.3.6.1.4.1.311.10.3.4)
Thumbprint Algorithm	sha1
Thumbprint	[Thumbprint of certificate]

Commerzbank AG group mail box certificates

Commerzbank Soft PSE Encryption	
X.509 Version	V3
Serial Number	[Certificate Serial Number]
Signature Algorithm	sha1RSA
Issuer	CN = Commerzbank AG Inhouse Sub CA 03 O = Commerzbank AG L = Frankfurt am Main C = DE
Key Length	2048
Valid from	[Start date and time]
Valid to	[End date and time]
Public Key	RSA (2048-Bit) Key Blob
Subject	E = <e-mail address group mail box> CN = <gropu mail box name> OU = Team Mailbox O = Commerzbank AG L = Frankfurt am Main C = DE
Key Usage	Key Encipherment
Subject Key Identifier	[corresponding private key]
Authority Key Identifier	d5 b6 fa fa 21 9f 06 eb c4 f2 cb f7 36 60 cb 3b 8c f0 3f a0
CRL Distribution Points	http://ca.commerzbank.com/cdp/coba_sub03.crl
Authority Information Access	http://ca.commerzbank.com/aia/coba_sub03.crt
Subject Alternative Name	<RFC 822 eMail address Gruppenpostfach>
Extended Key Usage	Secure e-mail (1.3.6.1.5.5.7.3.4)

Thumbprint Algorithm	sha1
Thumbprint	[Thumbprint of certificate]

7.1.1. Version number(s)

Commerzbank AG Inhouse Root CA and Commerzbank AG Inhouse Sub CA 03 issue X.509 Version 3 certificates.

7.1.2. Certificate extensions

Following certificate extensions are accounted for in certificates issued by Commerzbank:

Extension	Value	Cricitcal
Key Usage	Digital Signature, Certificate Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline), Key Encipherment, Non Repudiation	No
Subject Key Identifier	Unique number corresponding to the subject's public key. The key identifier method is used.	No
Authority Key Identifier	Unique number corresponding to the authority's public key. The key identifier method is used.	No
CRL Distribution Point	Contains the information where the current CRL can be obtained	No
Authority Information Access	Contains a link where additional information to the issuing CA can be obtained (ca issuers method)	No
Extended Key Usage	Contains application specific attributes/OIDs	No
Subject Alternative Name	Contains alternative Subject Names, such as eMail address or UPN	No
Certificate Issuance Policies	1.3.6.1.4.1.14978.5.1 (Commerzbank AG CP/CPS OID Referenz)	No

Following private certificate extensions are applied:

Extension	OID	Critical
Certificate Template Information	1.3.6.1.4.1.311.21.7	No
Application Policies	1.3.6.1.4.1.311.21.10	No

7.1.3. Algorithm Object Identifiers

- Commerzbank CAs create RSA key pairs (OID: 1.2.840.113549.1.1.1) according RFC 5280.
- Commerzbank CAs create signatures with sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) according RFC 5280.

7.1.4. Name forms

CA certificates issued by **Commerzbank AG Inhouse Root CA** obtain the full DN (Distinguished Name) in Subject Name and in the Issuer Name field. The DN is composed according to X.500 and contains the compontens in the following order:

CN = [Common Name],
O = [Organization],
L = [Locality],
C = [Country]

End-entity certificates issued by **Commerzbank AG Inhouse Sub CA 03** obtain the full DN (Distinguished Name) in Subject Name and in the Issuer Name field. The DN is composed according to X.500 and contains the compontens in the following order:

For **CoBa SC Authentication** certificates:
CN = [Common Name],
O = [Organization],
L = [Locality],
C = [Country]

For **CoBa SC Signature, CoBa SC Encryption** certificates:
E = [RFC 822 eMail Address],
CN = [Common Name],
O = [Organization],
L = [Locality],
C = [Country]

For **Commerzbank Soft PSE Encryption** certificates:
E = [RFC 822 eMail Address],
OU = [Organization Unit],
CN = [Common Name],
O = [Organization],
L = [Locality],
C = [Country]

7.1.5. Name constraints

Not applicable. There are no name constraints.

7.1.6. Certificate policy object odentifier

The Commerzbank AG Certificate Policy OID for the Root CA is: 1.3.6.1.4.1.14978.5.1

7.1.7. Usage of policy constraints extension

Not applicable.

7.1.8. Policy qualifiers syntax and semantics

The Commerzbank Certificate Policy Qualifier ID is: CPS.

- Commerzbank PKI OID:
- 1.3.6.1.4.1.14978.5.1

The Commerzbank CPS location is represented by an URL:

- http://ca.commerzbank.com/cps/cps.htm

7.1.9. Processing Semantics for critical certificate policies extension

Not applicable.

7.2. CRL profile

CRLs are issued in the scope of the Commerzbank Personen PKI. Issuance of deltaCRLs not planned for the Commerzbank Root CA.

Commerzbank CRL profiles comply with:

- ITU-T recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.

Commerzbank CRL profiles comply with:

- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
- RFC 5280 (succeeding RFC 3280): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

CRL base fields are defined as follows:

Field	**Value**
Version	See *7.2.1. Version Number*
Issuer	Contains the Distinguished Name of the issuing CA
This update	Time and date of CRL issuance.
Next update	Time and date of next CRL update.
Signature Algorithm	Designation of algorithm used to sign the certificate. See *7.1.3. Algorithm Object Identifiers*
Signature	CAs signature

Commerzbank AG Inhouse Root CA – CRL profile	
Field	**Value**
Version	X.509 V2
Issuer	CN = Commerzbank AG Inhouse Root CA O = Commerzbank AG L = Frankfurt am Main C = DE
This update / Valid from	[Time and date of CRL issuance]
Next update	[Time and date of next CRL update]
Signature Algorithm	sha1RSA
Extension	**Value**
Authority Key Identifier	8c f9 89 bf 7e 3c ca 24 31 cc 70 c6 95 9d 72 47 36 27 c8 67
CRL Number	[Unique increasing number per CRL]
CA Version	Starting from: V0.0
Next CRL Publish	[Time and date of next CRL publish]

Revoked Certificates	Value
Certificate Serial Number	[Serial Number of revoked Certificate]
Revocation Date	[Time and date of Certificate revocation]
Reason Code	Revocation Reason: unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL

Commerzbank AG Inhouse Sub CA 03 – CRL profile	
Field	**Value**
Version	X.509 V2
Issuer	CN = Commerzbank AG Inhouse Sub CA 03 O = Commerzbank AG L = Frankfurt am Main C = DE
This update / Valid from	[Time and date of CRL issuance]
Next update	[Time and date of next CRL update]
Signature Algorithm	sha1RSA
Extension	**Value**
Authority Key Identifier	d5 b6 fa fa 21 9f 06 eb c4 f2 cb f7 36 60 cb 3b 8c f0 3f a0
CRL Number	[Unique increasing number per CRL]
CA Version	Starting from: V0.0
Next CRL Publish	[Time and date of next CRL publish]
Revoked Certificates	**Value**
Certificate Serial Number	[Serial Number of revoked Certificate]
Revocation Date	[Time and date of Certificate revocation]
Reason Code	Revocation Reason: unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL

7.2.1. Version number(s)

The Commerzbank Root CA issues CRLs based on X.509 Version 2.

7.2.2. CRL and CRL entry extensions

CRL extensions can be obtained from the current Commerzbank Root CA CRL profile. See *7.2. CRL Profile*.

7.3. OCSP profile

Not applicable. OCSP is not supported by the Commerzbank Personen PKI.

7.3.1. Version number(s)

Not applicable.

7.3.2. OCSP extensions

Not applicable.

8. Compliance audit and other assessments

In the scope of the Commerzbank Personen PKI internal audits are performed to detect deviations of regular operation of the Commerzbank PKI to the provisions of the Commerzbank Certificate Policy and Commerzbank Certification Practice Statement (CP/CPS) and perform corrective actions, if any deviations are revealed.

8.1. Frequency or circumstances of assessment

Generally, internal audits and assessments are planned in regular intervals. Frequency and circumstances for assessments are defined by Commerzbank revision.

8.2. Identity/qualifications of assessor

Only internal Commerzbank AG employees are envisaged to perform a compliance audit. Auditing personnel should have know-how in security audits, in particular necessary knowledge about Public Key Infrastructures (PKI) and data center operation (ITIL certification) are required.

8.3. Assessor's relationship to assessed entity

The assigned compliance assessor is organizationally independent from the assessed entity, the Commerzbank AG Personen PKI (technology and processes).

8.4. Topics covered by assessment

Topics covered by assessment are defined by Commerzbank revision for each case. For circumstances, which require an assessment, certail topics can be defined in advance.

This includes:

- Key Management Operations
- Certificate Lifecycle Processes
- Data Processing Security and Operations

8.5. Actions taken as a result of deficiency

If deficiencies are detected, they have to be corrected in due time. For this, an action plan is developed, which describes necessary corrective actions.

After implementation of the action plan, an assessment must take place, checking if the actions taken have corrected the deficiencies. The Commerzbank IT management and the Commerzbank revision are informed about the results.

8.6. Communication of results

Audit/assessment results are confidential and are not to be published.

9. Other business and legal matters

This chapter deals with business, legal, and privacz matters of the Commerzbank Personen PKI.

9.1. Fees

Fees for services provided by the CAs operated by Commerzban AG can be learned from the internal charging table. It can be requested from the contact stated in chapter 1.5.2.

9.1.1. Certificate issuance or renewal fees

Detailed information can be learned from the internal charging table for the Commerzbank Personen PKI service.

9.1.2. Certificate access fees

Detailed information can be learned from the internal charging table for the Commerzbank Personen PKI service.

9.1.3. Revocation or status information access fees

Detailed information can be learned from the internal charging table for the Commerzbank Personen PKI service.

9.1.4. Fees for other services

Detailed information can be learned from the internal charging table for the Commerzbank Personen PKI service.

9.1.5. Refund policy

Detailed information can be learned from the internal charging table for the Commerzbank Personen PKI service.

9.2. Financial responsibility

9.2.1. Insurance coverage

There is no insurance coverage.

9.2.2. Other assets

Other assets are not covered.

9.2.3. Insurance or warranty coverage for end-entities

There is no insurance coverage for end-entities/subscribers.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

Each information about participants and applicants that is not covered by 9.3.2. is considered confidential. These information include amongst others business plans, marketing information, business partner information and all information that become known during registration.

9.3.2. Information not within the scope of confidential information

Every information, which is contained in issued certificates and CRLs explicitly (e.g. e-mail address) or implied (e.g. certification data) or can be derived from this data, is not considered confidential.

9.3.3. Responsibility to protect confidential information

Every CA operating in the Commerzbank Personen PKI is responsible to proctect confidential information.

9.4. Privacy of personal information

9.4.1. Privacy plan

Storage and Processing of personal information comply with legal privacy regulations.

9.4.2. Information treated as private

Every information about subscriber and applicant have to be treated as private.

9.4.3. Information not deemed private

Information in public certificates, like the Commerzbank certificate or the CA certificate, are not deemed private. This also applies to information contained in public CRLs.

9.4.4. Responsibility to protect private information

Commerzbank PKI operations is responsible to protect private information. A disclosure of private information can only take place in agreement with responsible units. Further details can be requested from GS-ITR 4.3.

9.4.5. Notice and consent to use private information

Subscribers consent to use of private information by a CA in the extend required for service provision. Furthermore, all information not considered private may be disclosed.

9.4.6. Disclosure pursuant to judicial or administrative process

Commerbank AG complies with legal privacy regulations in storage and processing of private information. A disclosure towards public authorities takes place only if a court order has been issued.

9.4.7. Other information disclosure circumstances

None.

9.5. Intellectual property rights

The intellectual property rights for the documentation issued in the scope of the Personen PKI lie with the Commerzbank AG.

9.6. Representations and warranties

9.6.1. CA representations and warranties

The Commerzbank AG CAs commit to follow the general provisions of the CP/CPS documentation.

9.6.2. RA representations and warranties

The Commerzbank AG RAs commit to follow the general provisions of the CP/CPS documentation.

9.6.3. Subscriber representations and warranties

Use of certificates by the subscriber has to comply with the "Commerzbank Richtlinien für den Gebrauch von Zertifikaten". Chapter 1.4. certificate usage defines appropriate and prohibited certificate/key uses. Furthermore, the subscriber has to fulfil his duties according certificate policy.

9.6.4. Relying party representations and warranties

Certificate use by relying parties has to comply with the applicable certificate policy of the party's organization. Those specify appropriate and prohibited certificate/key uses.

9.6.5. Representations and warranties of other participants

Not applicable. No other participants are allowed for.

9.7. Disclaimers of warranties

Generally there is no warranty. Commerzbank AG provides the necessary IT resources for PKI operation, but does not guarantee for availability.

9.8. Limitations of liability

Commerzbank AG assumes no liability for property or financial damage. Especially in case of improper or grossly negligently use of Commerzbank Personen PKI there is no liability towards third parties.

9.9. Indemnities

In case of improper use of the certificate or the underlying private key or in case of use of keys based on incorrect application data, Commerzbank AG is released from liability

9.10. Term and termination

9.10.1. Term

The current Commerzbank CP/CPS documentation becomes effective after publishment. The document is published on the URL specified in the certificate:

http://ca.commerzbank.com/cps/cps.htm

9.10.2. Termination

This document remains effective until

- it is replaced by a new version or
- the Commerzbank AG CA operation terminates.

9.10.3. Effect of termination and survival

None.

9.11. Individual notices and communications with participants

Individual notice of Commerzbank Personen PKI participants takes place by distribution and acceptance of „Commerzbank Richtlinien für den Gebrauch von Zertifikaten".

9.12. Amendments

Amendments and modifications to CP/CPS documentation falls to GS-ITR 4.3. Contact data is published in chapter 1.5.

9.12.1. Procedure for amendment

Not applicable.

9.12.2. Notification mechanism and period

Not applicable.

9.12.3. Circumstances under which OID must be changed

Not applicable.

9.13. Dispute resolution provisions

Not applicable.

9.14. Governing law

The Commerzbank Personen PKI is operated according the law of the Federal Republic of Germany. Jurisdiction is Frankfurt am Main, Federal Republic of Germany. This jurisdiction also applies for parties, whose residence or domicile is abroad or unknown.

9.15. Compliance with applicable law

Certificates issued by Commerzbank Personen PKI are not conformal with qualified certificates. Hence, the provisions and rules of the Signaturgesetz [SigG] are not applicable for Commerzbank Personen PKI operation.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

All provisions of the Personen PKI CP/CPS are valid between the CAs operated by Commerzbank AG and their subscribers. Issuance of a new version does not supersede all previous versions. Verbal agreements and subsidiary agreements are not allowed.

9.16.2. Assignment

Assignment is not allowed for.

9.16.3. Severability

If particular provisions of this CP/CPS body of rules and regulations is ineffective or if this body of rules and regulations is incomplete, the applicability of other regulations is not affected.

In lieu of the ineffective regulation, the regulation is considered applicable, which fulfils the whole purpose of the ineffective regulation. In case of incompleteness, a regulation that would have been arranged according the whole purpose of the contract is considered applicable.

It is expressively agreed upon that all provisions of this CP/CPS, which contain a limitation of liability, a disclaimer or limitation of warranty, or indemnity, are individual regulations and remain in effect independently from other regulations, and can be enforced independently thereof.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

Legal disputes resulting from operation of a CA by Commerzbank AG are subject to the laws of the Federal Republic of Germany.

Place of performance and exclusive jurisdiction is Frankfurt am Main, Federal Republic of Germany.

9.16.5. Force Majeure

Commerzbank AG assumes no liability for breach of duty, default, or non-fulfilment in the scope of this CPS, as they result from occurrences outlying its control, e.g. forde majeure, acts of war, epidemics, network breakdowns, fires, earthquakes, and other disasters.

9.17. Other provisions

None.