# COMMERZBANK - X.509 PKI

# COMMERZBANK PERSONS PKI

Certificate Policy (CP)
&
Certification Practice Statement (CPS)

**Version 1.3**

## Document Control:

| | |
|---|---|
| Title: | Commerzbank Persons PKI – Persons PKI<br>Certificate Policy (CP) & Certification Practice Statement (CPS) |
| Description: | Presentation of the processes and procedures of Commerzbank Persons PKI |
| RFC Schema: | RFC 3647 (Certificate Policy and Certification Practices Framework) |
| Author: | Roland Schuetz, Commerzbank AG, GS-TF, Cell Crypto Services |

## Version Control:

| Version | Date | Comment |
|---|---|---|
| 1.0 | 20.01.2011 | Release version 1.0 |
| 1.2 | 17.12.2020 | Revision and update, concretization for the person PKI (Persons CA) in accordance with QM31-7520 |
| 1.3 | 10.01.2022 | Revision Root CA |

# Contents

# 1. Introduction

## 1.1. Document Overview

Commerzbank Persons Public Key Infrastructure (in short: Persons PKI) is the part of Commerzbank Public Key Infrastructure (CoBa PKI), which is used to generate, issue, manage and reallocate cryptographic keys and person-bound X.509 certificates. The PKI people are divided into different SUB CAs, which serve different purposes. Commerzbank Inhouse SubCA 03 issues the certificates used to implement e-mail encryption and e-mail signature based on the S/MIME standard, as well as authentication to IT systems for natural persons. It also provides cryptographic keys and X.509 certificates for secure communication with group or resource mailboxes. The PKI persons also include other SubCAs that create personal certificates for purely Commerzbank internal purposes.

This document is a combination of the "Certificate Policy" (CP) and the "Certification Practice Statement" (CPS) of Commerzbank Persons PKI. The consideration here lies in SubCA03, which issues certificates for cross-purposes of Commerzbank. SubCAs, which serve purely internal purposes are not taken into account. The document structure is based on the recommendations specified in RFC 3647.

The term "Certificate Policy (CP)", defined in the X.509 standard, represents the entirety of the rules and specifications that determine the applicability of a certificate type. The purpose of a certificate policy is discussed in detail in RFC 3647 ("Certificate Policy and Certification Practices Framework").

In the context of the Persons PKI, the CP enables users of e-mail encryption, e-mail signature and associated validation services or those responsible for group post subjects to assess the extent to which the respective service can be trusted based on the certificates issued in the context of the supported applications.

In particular, a CP defines:

- The technical and organizational requirements of the systems and processes used for issuing certificates
- Which specifications apply to the application of the certificates as well as to the handling of the associated keys and signature creation units (e.g. smart cards)
- The importance of the certificates and associated applications, i.e. the security, the force of proof or the legal relevance of the ciphertexts or signatures generated with them

The concept of the Certification Practice Statement (CPS)" was developed by the American Bar Association (ABA) and is implemented in its Digital Signature Guidelines (ABA Guidelines). The CPS is a detailed description of the PKI certification operation of the respective organization. Organizations that operate one or more certification authorities typically also provide a CPS.

Within the framework of the PKI people, the CPS is an adequate means of presenting the individual transactions of the Persons PKI in itself and in particular the transactions in the direction of the certificate holders and other parties.

The central aspect of Commerzbank CP/CPS of the Persons PKI is **thus the determination of the trustworthiness** of issued certificates and the certification services.

By participating in the Commerzbank certification services, the respective certificate holder accepts the conditions and regulations listed in this document.

The distribution of this document is free of charge and is open to the public.

## 1.2. Document title and identification

Commerzbank OID is registered with IANA.ORG.
(see also 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 X.509 PKI services of Commerzbank AG

The title of this document is:

*"Commerzbank Persons PKI – Certificate Policy (CP) & Certification Practice Statement (CPS)"*

**COMMERZBANK CP/CPS OID:** 1.3.6.1.4.1.14978.5.1

**OID Description:** OID for 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 for Commerzbank Persons PKI –Certificate Policy & Certification Practice Statement

This document is available for the certificate s and other interested parties at the following URL:
http://ca.commerzbank.com/cps/cps.html

## 1.3. Participants and components of the Persons PKI

As mentioned at the beginning, Commerzbank Persons PKI is used to generate, issue, manage and reallocate X.509 certificates for the implementation of e-mail encryption and e-mail signature based on the S/MIME standard.

In the current version, it supports two types of S/MIME X.509 certificates:

- Personal e-mail traffic can be secured through "personal certificates" that are tied to natural persons. A distinction is made between a person encryption certificate and a person signature certificate. In this context, the individual is referred to as the certificate holder. The carrier medium for the private keys and the associated certificates are chip cards. These also serve as a signaling unit.
- Group certificates that are bound to group or resource mailboxes can be used to secure communication with these mailboxes. The PKI provides only group encryption certificates. The person responsible for the mailbox is referred to as the certificate trustee. The private keys and associated certificates are provided in the form of PFX files.

On the other hand, the Persons PKI is used to generate, issue, manage and reallocate X.509 certificates for the authentication of persons to IT systems. The required cryptographic keys are generated on a smart card, which also serves as a medium for the private key and the associated certificate. The certificates are referred to as personal authentication certificates.

### 1.3.1. Architecture of the Persons PKI

The Persons PKI, as part of Commerzbank PKI, consist of four functionally separate parts:

- **Certification Authority or Certification Authority:**
  The certification authority serves
  - … the creation or issue of certificates,
  - … the revocation of certificates,
  - … and restoring user keys.
- **Registrars or Registration Authorities:**
  The registrars serves
  - … the identification of users,
  - … the registration of users,
  - … requesting a certificate request for other users or groups / Resources and
  - … requesting a revocation request for certificates.
- **Revocation Services**
  The Revocation Services provide certificate revocation lists (CRLs), which list revoked certificates of the Persons PKI, to confidential parties.
- **Directory Service**
  The Directory Services are used to provide the certificates of the Persons PKI to other trusting parties.

The Persons PKI allows controlled issuance and management of certificates and smart cards, which are used as a personal carrier medium for cryptographic keys and associated certificates. The output and management are carried out by a central certificate and smart card management system.

Further information on the Persons PKI architecture can be requested. The contact information is from Chapter 1.5.2. Contact persons.

**Note:**

Other certification authorities are established in the Commerzbank PKI environment, but they have no external effect. Therefore, these CA components were not listed in the current CP/CPS description for Commerzbank Persons PKI.

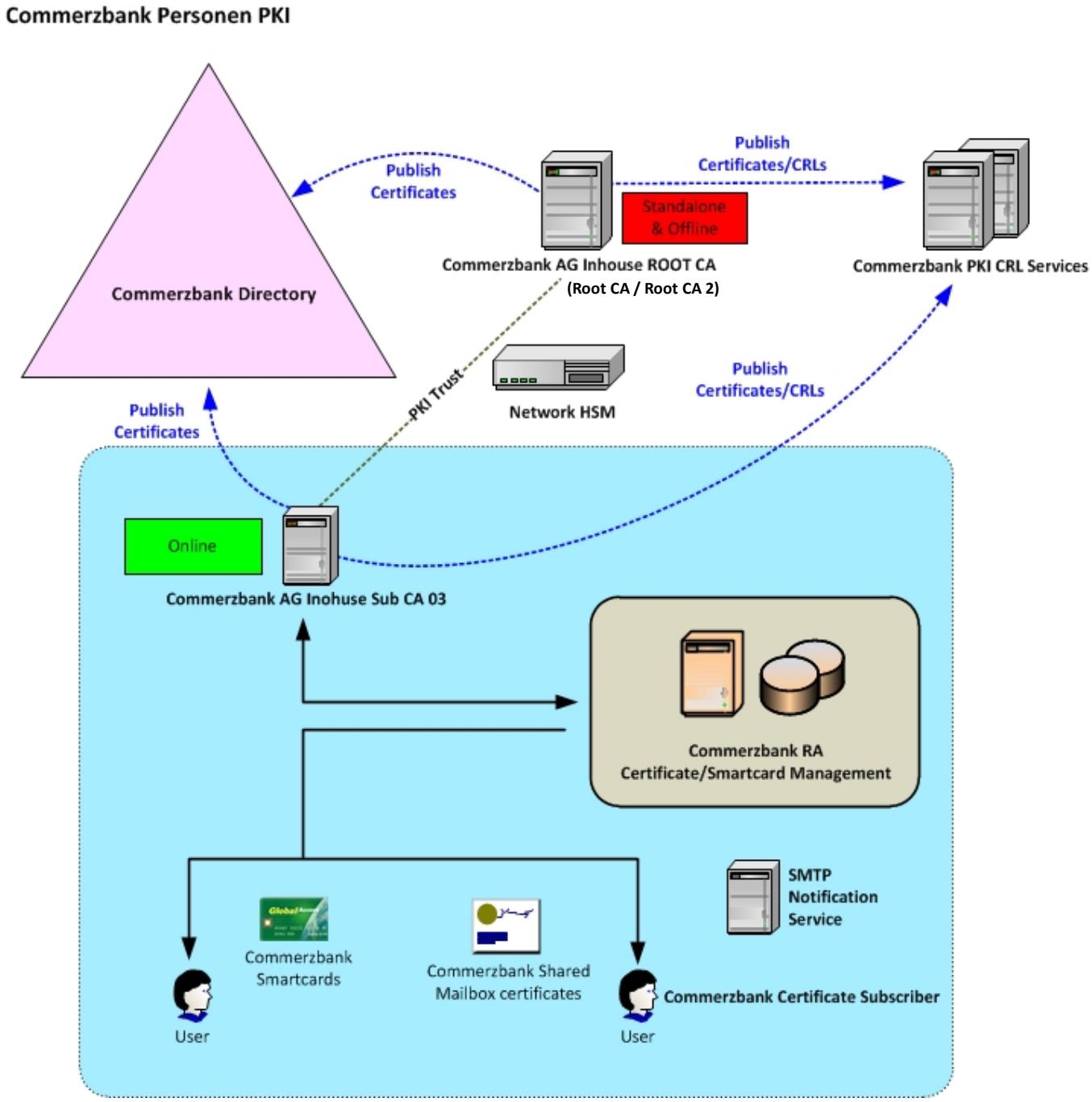


**Figure 1: Architecture of Commerzbank Persons PKI**

### 1.3.2. Certificate hierarchy and certification authority of the Persons PKI

The Commerzbank certification infrastructure is structured hierarchically and is scheduled at **Commerzbank AG Inhouse Root CA**. From an architectural point of view, there is a Root CA, from a technical point of view, the Root CA currently consists of two instances: **Commerzbank AG Inhouse Root CA** issued for stock certificates until September 2020 and **Commerzbank AG Inhouse Root CA 2** as an active CA root instance since September 2020. The person certification authority **(Commerzbank AG Inhouse Sub CA 03)** of the Persons PKI, including the associated certification services for the generation, issue and management of certificates, is directly subordinate to the root certification authority of Commerzbank PKI.

- **Commerzbank AG Inhouse Root CA 2** with a self-signed CA certificate.
  All crypto-graphic operations of Commerzbank Root CA 2 are executed by the HSM. Commerzbank Root CA 2 issues CA certificates and revocation lists for subordinated certification authority instances (Commerzbank AG Sub CA), as well as for itself.

  The following life periods are defined for this CA:
  - Root CA certificate: 30 years
  - Root CA CRLs: 4 months

  Commerzbank Inhouse Root CA 2's full DN is:

  **Commerzbank AG Inhouse Root CA 2**
  CN=Commerzbank AG Inhouse Root CA 2,
  O=Commerzbank AG,
  L=Frankfurt/Main,
  C=DE

- **Commerzbank AG Inhouse Root CA** with a self-signed CA certificate.
  All cryptographic operations of Commerzbank Root CA are executed by the HSM. Commerzbank Root CA was replaced by Commerzbank Root CA 2 in September 2020. It is no longer used to issue new certificates but is still used to verify inventory certificates and issue revocation lists for subordination CA instances (Commerzbank AG Sub CA).

  The following life periods are defined for this CA:
  - Root CA certificate: 30 years
  - Root CA CRLs: 4 months

  Commerzbank Inhouse Root CA's full DN is:

  **Commerzbank AG Inhouse Root CA**
  CN=Commerzbank AG Inhouse Root CA,
  O=Commerzbank AG,
  L=Frankfurt/Main,
  C=DE

- **(Online) Commerzbank AG Inhouse Sub CA 03** with a certificate issued by Commerzbank Root CA 2 (or the Root CA for older certificates). Commerzbank AG Inhouse Sub CA 03 is connected to the production network and maintains a dedicated connection to the Network HSM. All cryptographic operations of Commerzbank AG Inhouse Sub CA 03 are performed by the HSM.

Commerzbank Sub CA 03 issues end entity and revocation lists for the certificate holders. Specifically, these are personal encryption certificates, personal signing certificates, personal authentication certificates, and group encryption certificates.

The following life periods are defined for this CA:

- Sub CA 03 certificate: 7 years
- Sub CA 03 CRLs: 14 days

The complete DN of Commerzbank Inhouse Sub CA 03 is:

**Commerzbank AG Inhouse Sub CA 03**

CN=Commerzbank AG Inhouse Sub CA 03,
O=Commerzbank AG,
L=Frankfurt/Main,
C=DE

### 1.3.3. Registrars

For the purposes of this document, the registrars are the entities that collect the identity information of the certificate holders or the certificate trustee, verify their identity, and, if the identity is positive, request the certificate creation from the certification authorities. In addition, they serve as issuing points for certificates (and, if necessary, cryptographic keys) in the form of personalized smart cards in the sense of local registration authorities (LRA).

Certificate application for the certificate holders or certificate holders is carried out via a registration tool, which enables the controlled generation of cryptographic keys on smart cards, the transfer of the generated public keys from Smart Cards to the person certification authority and the transfer of certificates to Smart Cards. In addition, this tool organizes the entire lifecycle management of certificates and smart cards.

The initial creation is not carried out by the certificate holder or the certificate trustee himself. This is the responsibility of employees of the PKI people.

### 1.3.4. Certificate holder and certificate trustee

Certificate holders within the scope of the PKI are Commerzbank full-time employees, part-time employees and, if necessary, business partners and external employees to whom S/MIME certificates or person authentication certificates are assigned by the Persons PKI. Key generation and certificate output are not under the control of the certificate holder but are the responsibility of the Persons PKI.

Certificate trustees are Commerzbank full-time employees and part-time employees who are assigned S/MIME certificates not for themselves but for group or resource mailboxes.
Certificate holders and certificate holders consume certificates and PKI services of the Persons PKI.

### 1.3.5. Trusting parties

For the purposes of this document, trusting parties are all persons and systems that securely communicate or authenticate on the basis of certificates issued by the Persons PKI.
Trusting parties consume PKI services and, in particular, validate signatures using certificates and revocation lists provided through Directory Services.

## 1.4. Application of certificates

The use of private keys and certificates is the responsibility of the certificate holder or the certificate trustee and the trusting party.

### 1.4.1. Allowed use of certificates

The certificates issued under these CP/CPS are to be issued by the certificate holder for **authentication** (e.g. Windows logon), and to **encrypt and sign e-mail** messages. In the case of group mailboxes, the use of the certificates is intended to implement the encryption of e-mails.

The following tables describe the scope of the certificates issued by the Persons PKI:

**Issued by Commerzbank AG Inhouse Root CA (Root CA and Root CA 2):**

| Certificate type | Scope of the issued certificate |
|---|---|
| Certification Authority | ROOT CA Certificate for self-signed (root) CAs |

**Issued by Commerzbank AG Inhouse Root CA (Root CA and Root CA 2):**

| Certificate type | Scope of the issued certificate |
|---|---|
| Subordinate Certification Authority | CA certificate for subordinated certification authorities |

**Issued by Commerzbank Inhouse Sub CA 03:**

| Certificate type | Scope of the issued certificate |
|---|---|
| Coba SC Authentication<br>(People authentication certificate) | Smart Card authentication certificate for login,<br>For example Windows Logon |
| Coba SC Encryption<br>(People encryption certificate) | Smart Card Encryption certificate for encryption, for example, for encryption of e-mails |
| Coba SC Signature<br>(People Signature Certificate) | Smart Card Signature certificate for the electronic signature, e.g. for the signing of e-mails |
| Commerzbank Soft PSE Encryption<br>(System Encryption Certificate) | Software Encryption certificate for encrypting e-mails for group mailboxes. |
| "Certificates for the certificate management system" | In addition, for the operation of the certificate management system, software certificates have become created for technical usage within the system |

### 1.4.2. Invalid use of certificates

The certificate usage of person certificates within the scope of the Persons PKI is limited to the in 1.4.1 Associated Use Purposes. The use of the certificates for private use as well as the use of the certificates for other purposes other than 1.4.1 is not permitted.

To protect Commerzbank CP/CPS compliance, any change or extension of the certificate application must be notified immediately to Commerzbank PKI Administration.

## 1.5. Policy management

### 1.5.1. Organization

Commerzbank AG is the responsible organization for policy management.

**Commerzbank AG**
60261 Frankfurt am Main
Germany

### 1.5.2. Contacts

Responsible unit for Commerzbank Persons PKI:

**GS-TF Cloud Foundation, cell Crypto Services**
(Short "Crypto Services")
Theodor-Heuss-Allee 100
D-60486 Frankfurt/Main

cryptoservices@commerzbank.com

Contacts:

**Laurent Koehler / Roland Schuetz**
Commerzbank AG
GS-TF Cloud Foundation
Cell Crypto Services
Theodore-Heuss-Allee 100
D-60486 Frankfurt/Main
Tel: + 49 69 136 42814 / +49 69 136 21880

### 1.5.3. Responsible persons for the CPS

Commerzbank AG, GS-TF Cloud Foundation, Crypto Services is responsible for compliance with the certification operation and the certificate guidelines in accordance with the CP/CPS and accompanying documentation.

The contact persons for compliance with the CP/CPS are in section 1.5.2. Contact persons listed. These are also the people responsible for this document.

### 1.5.4. CPS approval process

Commerzbank AG, GS-TF Cloud Foundation, Crypto Services is responsible for the release of these CP/CPS. The CP/CPS documentation is continually checked for compliance.

## 1.6. Definitions and abbreviations

**ABA (American Bar Association)** - Association of American auditors

**Abstract Syntax Notation (ASN.1)** - abstract syntax notation number 1, data description language

**C (Country)** - State object (part of X.500 Distinguished Name), for Germany C=DE

**Certification Authority (CA)** — Certificate Authority

**CN (Common Name)** - Name object (part of X.500 Distinguished Name)

**CP (Certificate Policy)** - Certificate Policy

**CPS (Certification Practice Statement)** - Certification Authority

**Certificate Revocation List (CRL)** - List in which a CA publishes certificates issued by it that are revoked but not expired

**Certificate Signing Request (CSR)** — signed certificate request

**Distinguished name (DN)** – Unique name is based on X.500 naming

**Domain Name System (DNS)** - the default for Internet names

**Federal Information Processing Standard (FIPS)** —The U.S. government's cryptographic standard

**Hardware Security Module (HSM)** - Hardware component that securely stores and processes security-related information such as data and cryptographic keys

**Internet Engineering Task Force (IETF)** - Project group for the technical development of the Internet. Specifies quasi-standards in the form of RFCs

**Internet Protocol (IP)** - Internet protocol

**ISO (International Organization for Standardization)** - International Standards Agency

**ITU (International Telecommunications Union)** – a standardization body, has also specified X.509

**Lightweight Directory Access Protocol (LDAP)** — Access protocol for directory services

**NIST (National Institute of Standards and Technology)** – The United States standardization body

**O (Organization)** - Object for the organization (Part of X.500 Distinguished Name)

**OID (Object Identifier)** – Object Identifier, unique reference to objects in the OID namespace

**OU (Organizational Unit)** - Object for the organizational unit (Part of X.500 Distinguished Name)

**Personal Identification Number (PIN)** - A secret number used to authenticate an individual, e.g. against a chip card

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

**Public Key Infrastructure (PKI)** – Describes technology, processes, and participants in asymmetric cryptography

**Public Key Infrastructure Exchange (PKIX)** – a series of IETF specifications in the environment of Digital certificates according to X.509 specification

**RA (Registration Authority)** - Registrar

**RFC (Request for Comment)** – quasi Internet standard issued by the IETF

**RSA** - asymmetric cryptographic technique that can be used for encryption and signing. (Named after Rivest, Sharmir, Adleman)

**Uniform Resource Locator (URL)** - Resources Location on the Internet

**X.500** — Protocols and Services for ISO-compliant directories

**X.509** – Authentication method for X.500 directories

**X.509 v3** – current valid PKI certificate standard

# 2. Publishing and information services

## 2.1. Directory and information services

Persons PKI uses an internal directory service to provide certificates for secure e-mail communication. The required recipient certificates (person or group encryption certificates) are managed by the Persons PKI.

A web-based service is used as an information service to provide public information, such as Commerzbank CA certificates, CRLs, and CP/CPS documentation. Similarly, CA information is published in the Commerzbank directory service (Commerzbank Active Directory), with the exception of the CP/CPS documentation.

## 2.2. Publish certification information

The publication of the encryption certificates (e-mail recipient certificates) is automated by the Persons PKI in the local directory service. No user intervention is required. External recipient certificates for secure e-mail communication are provided through an upstream exchange of recipient certificates.

The continuous publication of the certificate revocation lists (CRLs) on the Commerzbank PKI-CRL web servers is carried out automatically by Commerzbank AG Inhouse Sub CA 03. Commerzbank AG Inhouse Root CA (Root CA and Root CA 2) is published manually by employees of GS-TF Cloud Foundation, cell Crypto Services on the web servers. This is due to the network separation or offline operation of Commerzbank Root CA. The Commerzbank CA certificates and the CP/CPS documentation are released by GS-TF Cloud Foundation, cell Crypto Services and set up on the corresponding PKI web servers.

**The following publication locations are planned:**

| | |
|---|---|
| *Commerzbank AG CP and CPS:* | http://ca.commerzbank.com/cpcps.en.html |
| *Commerzbank AG CRLs:* | http://ca.commerzbank.com/cdp/coba_root.crl |
| | http://ca.commerzbank.com/cdp/coba_rootca2.crl |
| | http://ca.commerzbank.com/cdp/coba_sub03(1).crl |
| | http://ca.commerzbank.com/cdp/coba_sub03(2).crl |
| *Commerzbank AG CA Certificates:* | http://ca.commerzbank.com/aia/coba_root.crt |
| | http://ca.commerzbank.com/aia/coba_rootca2.crt |
| | http://ca.commerzbank.com/aia/coba_sub03(1).crt |
| | http://ca.commerzbank.com/aia/coba_sub03(2).crt |

## 2.3. Publish Interval

The Commerzbank Certificate Policies and the Certification Practice Statements are published after they have been created or updated.

The Commerzbank CA certificates are published once after the Commerzbank certification authorities have been installed. A new publication is only carried out when the CA certificates expire or renew.

CRL or revocation lists are generated at the specified publication interval and are immediately published on the PKI CRL Web servers:

*CRLs issued by the root CA:* 3 months with an overlap of 1 month

*CRLs issued by root CA 2:* 3 months with an overlap of 1 month

*CRLs issued by Sub CA 03:* Weekly with 7-day overlap

The Commerzbank Registration Authority Officer publish interval of the external recipient certificates is defined according to a defined process. Appropriate process information can be obtained from GS-TF, Cloud Foundation, Cell Crypto Services if required.

## 2.4. Access to information services

Access to Commerzbank CA certificates, CRLs and the CP/CPS documentation is not restricted and is therefore public. See also publication locations in section 2.2 Publish certification information.

# 3. Identification and authentication

## 3.1. Names

### 3.1.1. Name form

The X.500 Distinguished Name (DN) in Commerzbank's CA certificates is specified as shown in the following tables. The use of DNS for naming in the Subject Name Field allows the unique naming of certification authorities within Commerzbank AG

The naming scheme is identical for all certificates issued by Commerzbank AG Inhouse Root CA and follows the rules below:

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

In actual implementation of the CA infrastructure, not all (name) attributes are defined, as the significance and uniqueness of the names for the CA with the attributes required for them is considered sufficient.

#### 3.1.1.1. Commerzbank AG Inhouse Root CA 2 DN

The X.500 DN of the self-signed Commerzbank AG Inhouse Root CA 2 is:

| Attributes | Value |
|---|---|
| Email | *** |
| Common Name (CN) | Commerzbank AG Inhouse Root CA 2 |
| Organization Unit | *** |
| Organization | Commerzbank AG |
| Locality | Frankfurt am Main |
| State or Province | *** |
| Country | DE |

#### 3.1.1.2. Commerzbank AG Inhouse Root CA DN

The X.500 DN of the self-signed Commerzbank AG Inhouse Root CA is:

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

#### 3.1.1.3. Commerzbank AG Inhouse Sub CA 03 DN

The X.500 DN in the certificate of Commerzbank AG Inhouse Sub CA 03 is:

| Attributes | Value |
|---|---|
| Email | *** |
| 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 Commerzbank AG Inhouse Sub CA 03 and follows the following rules and regulations:

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

#### 3.1.1.4. Commerzbank AG Smart Card Certificates DN

The X.500 DN in the **Coba SC Authentication** certificate issued by Commerzbank Inhouse Sub CA 03 is:

| Attributes | Value |
|---|---|
| Email | *** |
| Common Name (CN) | <Common name of Commerzbank user > |
| Organization Unit | *** |
| Organization | Commerzbank AG |
| Locality | Frankfurt am Main |
| State or Province | *** |
| Country | DE |

**Note:** The Commerzbank Smart Card certificate for authentication is only used in the Commerzbank infrastructure and is not published externally.

The X.500 DN in the **Coba SC Encryption** certificate issued by Commerzbank Inhouse Sub CA 03 is:

| Attributes | Value |
|---|---|
| Email | <Email address of Commerzbank user> |
| Common Name (CN) | <Display name of Commerzbank user> |
| Organization Unit | *** |
| Organization | Commerzbank AG |
| Locality | Frankfurt am Main |
| State or Province | *** |
| Country | DE |

The X.500 DN in the **Coba SC Signature** certificate issued by Commerzbank Inhouse Sub CA 03 is:

| Attributes | Value |
|---|---|
| Email | <Email address of Commerzbank user> |
| Common Name (CN) | <Display name of Commerzbank user> |
| Organization Unit | *** |
| Organization | Commerzbank AG |

| | |
|---|---|
| Locality | Frankfurt am Main |
| State or Province | *** |
| Country | DE |

#### 3.1.1.5. Commerzbank AG Certificates for Group mailboxes DN

The X.500 DN in the **Commerzbank Soft PSE Encryption** certificate issued by Commerzbank Inhouse Sub CA 03 is:

| **Attributes** | **Value** |
|---|---|
| Email | < Group mailbox email address> |
| Common Name (CN) | <Group mailbox name> |
| Organization Unit | Team mailbox |
| Organization | Commerzbank AG |
| Locality | Frankfurt am Main |
| State or Province | *** |
| Country | DE |

### 3.1.2. Requirement for meaning of names

The DN must uniquely identify the certificate holder or group mailbox. If the DN is not sufficient, the Subject Alternative Name can also be used to maintain the uniqueness of a name. The following regulations are effective when assigning names:

- Certificates may only be issued to a valid name of the certificate holder or certificate trustee.
    - For person authentication certificates for users, it is the common name of the user and the user principle name (UPN) in the Subject Alternative Name field of the certificate holder.
    - For user personal encryption and personal signature certificates, it is the last name, first name in the common name, and the email address in the Subject Alternative Name field of the certificate holder.
    - For group mailbox encryption certificates, it is the group mailbox name in the Common Name and the group mailbox email address in the Subject Alternative Name field.

- The DN of the Commerzbank certification authorities is formed by the name objects Common Name, Organization, Locality and Country. An uniqueness of the DN must be ensured with this available name objects. The DN of the authentication certificates is formed by the name objects Common Name, Organization, Locality and Country. Uniqueness of the DN must be ensured with this available name objects.
- The DN of the person encryption and person signature certificates is formed by the name objects Common Name, Organization, Locality, Country and the e-mail address of the Commerzbank user. Uniqueness of the DN must be ensured with this available name objects.
- The DN of the group encryption certificates for group mailboxes is formed by the Common Name, Organization Unit, Organization, Locality, Country name objects and the e-mail address of the group mailbox. Uniqueness of the DN must be ensured with this available name objects.
- The alternate name in the encryption and signature certificates contains the email address of the certificate holder in the form Vorname.Nachname@commerzbank.com, or Vorname.Nachname@partner.commerzbank.com for external employees.
- Each certificate is assigned a unique serial number, which enables a unique and unchangeable assignment to the certificate holder.

### 3.1.3. Anonymity and pseudonym of certificate holders

Apart from technical accounts (service certificates for the management system) or group certificates for group mailboxes, natural certificate holders (persons) are not anonymous, nor are pseudonyms used to identify certificate holders. Each certificate holder can therefore be assigned the certificates uniquely.

### 3.1.4. Rules for interpreting different name forms

The identified DN in the certificate profile follow the X.500 standard.
The Commerzbank e-mail addresses and UPN entries in the certificate profile follow the RFC 822 rules and regulations. UPN name information must be UTF-8 encoded.

### 3.1.5. Uniqueness of names

The complete DN in the certificates issued by Commerzbank permits the uniqueness of names, both of the Commerzbank certification authorities and the names for the Commerzbank certificate holders.

An additional identifier in the alternate name field, the unique Commerzbank
E-mail address, user UPN information and a unique serial number in the certificates, supports uniqueness.

### 3.1.6. Recognition, authentication and role of trademarks

Generally, the DN is limited to natural persons and therefore has no relevance in the recognition of trademarks. In principle, the certificate holder and also the certification authority operator are obliged to ensure that the protection of the trademarks is guaranteed by the automated issuing of person and group certificates.

## 3.2. Identity verification on new request

### 3.2.1. Procedures for checking the possession of private keys

In the case of person certificates, the key pairs for signing and authentication are generated on a smart card. The key pairs for group and resource mailboxes are generated on the requesting machine of the certificate trustee.

Private key ownership is provided in all of the above cases by signing the PKCS#10 certificate request with the private key. The Certificate Signing Request or CSR serves as proof of ownership for the private key.

The key pairs of Commerzbank certification authorities and the key pairs for person encryption certificates are generated by the Hardware Security Module. The private key ownership is also provided here by signing the PKCS#10 certificate requests with the private key. The Certificate Signing Request or CSR is the proof of ownership and the basis for checking private keys.

### 3.2.2. Authentication of the organization

Not applicable.

Only personal, individual certificates for Commerzbank employees or certificates for Commerzbank group mailboxes are issued. No certification of employees from other organizations takes place. External employees who have a Commerzbank e-mail address working longer term with Commerzbank can temporarily apply for person certificates for secure e-mail communication, but they are only valid for the context of Commerzbank.

### 3.2.3. Authentication of the certificate holder and trustee

For initial issuance of certificates to users and group mailboxes, identity verification and authentication is performed by the registrar.

In the case of personal certificates, the person is authenticated using a single PIN, which is checked to personalize the Smart Card.

The initial issue of group certificates for group and resource mailboxes to the certificate trustee is automated via a web page. This website is preceded by authentication at Commerzbank-AD. In this case, the entry of the ComSI-ID and the password of the certificate sender serves as identification and authentication.

For more details on identity verification and authentication, refer to the process flow for issuing smart cards and issuing certificates for group mailboxes.

### 3.2.4. Unverified certificate holder information

Only the information of the certificate holder that is required for the identification and authentication of the certificate holder is checked. No other information from the certificate holder will be taken into account.

### 3.2.5. Review eligibility for claim

Before issuing and issuing personal certificates and certificates for group mail subjects, the authorization of the respective applicant is checked.

In both cases, the approval of the line manager must be available.

For more details on checking permission, refer to the process for issuing smart cards and issuing certificates for group mailboxes.

#### 3.2.6. Criteria for cross-certification and interoperability

Not applicable.

No cross-certification with other organizations is currently being implemented or planned.

## 3.3. Identification and authentication during certificate renewal

#### *3.3.1.* Identification and authentication during routine certificate renewal

The renewal of person and group certificates is automated by the Persons PKI and the associated management systems. Affected certificate holders or certificate trustees will be notified by e-mail about the renewal. For renewal, successful identification and authentication of the certificate management system using a Windows user ID and a one-time-password of the respective certificate holder or certificate trustee is sufficient.

**Note:** A pin is also required for authentication on the smart card.

#### *3.3.2.* Identification and authentication for certificate renewal after certificate recall has been completed

The identification and authentication of a certificate renewal after a revocation of the respective certificate corresponds to the identification and authentication of the initial registration.

## 3.4. Identification and authentication for certificate recall

In principle, certificate holders and certificate holders can withdraw their own certificates assigned to them. This can also be initiated by the respective line managers (e.g. in the event of an employee leaving the company). For the recall itself, the registration office (where applicable, LRA) must be contacted and a corresponding request completed.

Detailed information on the application system can be obtained from Crypto Services if required.

# 4. Operational requirements for the certificate life cycle

This chapter describes the operational aspects of the certificate life cycle.

## 4.1. Certificate request

**Certificate application for Commerzbank Person Certificates**:

The initial application and renewal of Smart Card-based personal certificates is controlled by a certificate and smart card management tool. User-related certificates are provisioned on a Smart Card. The certificate lifecycle management and Smart Card management are subject to the control of the management system.

**Certificate application for Commerzbank Group certificates**:

The initial application and extension of group certificates for group and resource mailboxes is controlled by a certificate management tool. Certificate lifecycle management is controlled by the management system.

Further information on the certificate application can be obtained from Crypto Services if required.

### 4.1.1. Eligible for a certificate

The following are eligible for a person certificate:

1. All Commerzbank employees,
2. External employees who are employed at Commerzbank for a longer period of time. (Smart cards are only issued temporarily for external employees.)

The persons responsible for a group or resource mailbox are authorized to apply for a group certificate.

### 4.1.2. Delivery process and responsibilities

The issue of person certificates and group certificates is carried out by Commerzbank Persons PKI. Responsibility for the output process lies with the GS-TF Cloud Foundation, cell Crypto Services.

Once the request processing processes have been completed successfully, the certificate management system is used to initiate the creation of the certificates and to initiate the distribution.

A "tunnel" is set up for the respective smart card for the smart card carrier medium. This then transfers the private key for e-mail encryption and the issued certificates (signature, authentication and encryption).

In the case of group certificates, the certificate is provided for download via the PKI management system web page.

A detailed description of the output process and the technical implementation can be obtained from Crypto Services if required.

## 4.2. Process for processing applications

As with certificate applications, Smart Card-based personal and group certificate request processing is a process controlled by the certificate management system.

#### 4.2.1. Perform identification and authentication

The applicant is identified and authenticated on the basis of valid Commerzbank domain accounts. This applies both to the application for Smart Card-based person certificates and to the application for group certificates for Commerzbank group mailboxes.

#### 4.2.2. Accept or reject certificate requests

A certificate request is accepted if a valid line manager approval is available. This means that the associated line manager is the requester, a cost center is named and a signature is available on the request. In exceptions, an e-mail confirmation with a digital signature is accepted. If such a request is not available, the request will be rejected.

#### 4.2.3. Processing time of certificate requests

The certificate requests are processed in a controlled manner by the certificate management system. This procedure allows the certificate to be issued to the applicant immediately after the certificate request has been verified.

This results in immediate processing in both of the above applications. Upstream processes are not taken into account, which can extend the processing time.

### 4.3. Certificate output

As with the certificate request, the certificate output of person certificates and group certificates for group mailboxes is a controlled process by the certificate management system.

#### 4.3.1. Activities of the CA on certificate issue

Before issuing the certificates to the certificate holders, the following steps are carried out on the CA side.

- Validation of the certificate request by the CA policy module
    - When output is controlled by the certificate management system, validation is performed by the certificate management policy module.
- Archiving of issued certificates and certificate requirements in the Commerzbank AG Inhouse Sub CA 03 database.
- Archive the issued certificate information and request flow in the certificate management system database. In addition, smart card-relevant information, such as the PUK (Admin Key), as well as additional information, is stored in this database in an encrypted format.
- For personal encryption certificates, the associated key pairs are generated in the CA and archived in the Commerzbank AG Inhouse Sub CA 03 database.
- The issuing of certificates for the applicant is controlled via the certificate management system.

#### 4.3.2. Issue notification of the certificate holders by the CA

An issue notification by the issuing CA and additionally by Commerzbank Trustcenter takes place.

### 4.4. Certificate acceptance

As with the certificate application, the acceptance of person certificates and group certificates for group mailboxes is a controlled process by the Commerzbank certificate management system.

The detailed procedures for accepting user certificates can be found in the process procedures for issuing smart cards and can be obtained from Crypto Services if required.

### 4.4.1. Certificate acceptance procedure

Certificate acceptance is:

- Group certificate acceptance is considered complete when the issued certificate has been downloaded and the certificate management system has logged the output process as "completed".
- Certificate acceptance for Smart Cards-based Personal Certificates is considered complete when the Smart Card Management System has reported the successful transfer of keys and certificates and the Certificate Management System has logged the output process as "completed".

### 4.4.2. Publication of certificates

The publication of the encryption certificates is automated by the Persons PKI into the local directory service once the certificate acceptance is completed. User intervention is not necessary.

The publication of Commerzbank CA certificates for Commerzbank AG Inhouse Root CA , Commerzbank AG Inhouse Root CA 2 and Commerzbank AG Inhouse Sub CA 03 is executed manually on the PKI Web servers by Crypto Services. This also applies to the renewal of the above-mentioned CA certificates.

### 4.4.3. Output notification of other entities by the CA

No output notification to other entities by Commerzbank CAs will take place.

## 4.5. Key pair and certificate usage

Basically, the use of the key pair is intended for the authentication and encryption/decryption of information and for the creation/validation of signatures.

### 4.5.1. Use of the private key and certificate by the certificate holder

The use of the certificates by the certificate holder or the certificate trustee must follow the Commerzbank certificate guidelines. In Chapter 1.4. The scope of application of certificates is defined for the permissible and illegal applications of the keys or certificates. The permitted use is stored in the certificate as an attribute.

In addition, when using the private keys, the certificate holder must fulfill his obligations as defined in the Commerzbank policy for smart cards.

**Use of Commerzbank Smart Card-based personal certificates:**

The use of Commerzbank Smart Card-based personal certificates extends beyond authentication, to encryption and the creation of a digital signature in the context of secure e-mail communication.

Detailed use cases can be found in the Commerzbank certificate profiles.

The following technical framework conditions must be emphasized:

1. Personal certificates and associated private keys are available on the Smart Card.
2. The management and issue of Commerzbank Smart Card-based personal certificates is the responsibility of the central certificate management system.

3. Associated CPS, CRL, and CA certificates are published.
4. S/MIME e-mail certificates are published in the Commerzbank directory service.
5. Key archiving of encryption keys and all issued certificates is established.

Further information on the application area of the Persons PKI can be obtained from Crypto Services if required.

**Use of Commerzbank Group Certificates for Group mailboxes:**

The use of group certificates is used exclusively for the encryption of e-mails for group mailboxes. Further uses are excluded.

The following technical framework conditions must be emphasized:

1. Certificates and private keys for group mailboxes exists only as Software (Soft PSE)
2. The management and issue of certificates for group mailboxes is the responsibility of the central certificate management system.
3. Associated CPS, CRL, and CA certificates are published.
4. Certificates for group mailboxes are published in the Commerzbank directory service.
5. Key archiving of encryption keys and issued certificates for group mailboxes is established.

Further information on the application area of the Persons PKI can be obtained from Crypto Services if required.

### 4.5.2. Use of the private key and certificate by trusting parties

The use of the certificates by trusting parties must comply with the assigned certificate policies of his organization. The permissible and illegal applications of the keys or certificates are defined there.

It is assumed that this will take into account the usage specified in the certificate.

## 4.6. Certificate renewal

Within the framework of Commerzbank Persons PKI, the certificate renewal takes place exclusively with key change. Certificate lifetime renewal with consistent key pairs is not planned. Therefore, all of the following items under 4.6 are not applicable to Commerzbank Persons PKI.

### 4.6.1. Circumstances for certificate renewal

Not applicable.

### 4.6.2. Certificate Renewal Request

Not applicable.

### 4.6.3. Perform a certificate renewal

Not applicable.

### 4.6.4. Renewal notification for the certificate holder

Not applicable.

#### 4.6.5. Procedure for accepting certificate renewal

Not applicable.

#### 4.6.6. Publication of the renewed certificate by the CA

Not applicable.

#### 4.6.7. Renewal notification of other entities by the CA

Not applicable.

## 4.7. Certificate renewal with key change

Within the framework of Commerzbank Persons PKI, the certificate renewal only takes place with key change. The content of the certificate (data adaptation) is to be adapted as personal data such as e-mail address and names can change over the runtime. All of the following items under 4.7. are not applicable to Commerzbank Persons PKI.

#### 4.7.1. Circumstances for certificate renewal with key change

Not applicable.

#### 4.7.2. Certificate Renewal Request with Key Change

Not applicable.

#### 4.7.3. Perform a key-change certificate renewal

Not applicable.

#### 4.7.4. Renewal notification for the certificate holder

Not applicable.

#### 4.7.5. Procedure for accepting certificate renewal with key change

Not applicable.

#### 4.7.6. Publication of the renewed certificate by the CA

Not applicable.

#### 4.7.7. Renewal notification of other entities by the CA

Not applicable.

## 4.8. Certificate renewal with key change and data customization

Within the framework of Commerzbank Persons PKI, the certificate renewal takes place exclusively with key change. Technically, it is the replacement of a certificate with a certificate with a new validity period and for a new public key (or also new private key) and possible adaptation of content data.

#### 4.8.1. Circumstances for a certificate renewal with key change and data customization

Certificate renewal with key change and data modification can be requested if at least one of the following conditions is met:

- The current certificate's validity period has expired or is about to expire.
- The old certificate has been revoked.

- The information contained in the certificate is incorrect.
- The old key can or may no longer be used because it has (possibly) been compromised.
- The validity period of the current certificate or the current key length no longer provides sufficient security.
- The certificate can no longer be used technically (loss of the private key or no access to private keys).

#### 4.8.2. Certificate Renewal Request with Key Change

All certificate holders and certificate holders to whom a valid certificate has been assigned by the Persons PKI are entitled to apply.

#### 4.8.3. Perform a certificate renewal with key change and data customization

The process is similar to the initial creation. The PKI performs the certificate renewal with key changes of Smart Card-based person certificates and group certificates for group mailboxes in a controlled manner by the certificate and smart card management system.

#### 4.8.4. Renewal notification for the certificate holder

In the case of controlled issuance and renewal by the Certificate and Smart Card Management System, a renewal notification is sent to the applicant by e-mail. The renewal notification is sent to the parties within the renewal interval.

#### 4.8.5. Procedure for accepting certificate renewal with key change with data customization

The certificate acceptance takes place as well as during the application process by the Persons PKI.

- Group certificate acceptance is considered complete when the issued certificate has been downloaded and the certificate management system has logged the output process as "completed".
- Certificate acceptance for Smart Cards-based Personal Certificates is considered complete when the Smart Card Management System has reported the successful transfer of keys and certificates and the Certificate Management System has logged the output process as "completed."

#### 4.8.6. Publication of the renewed certificate by the CA

The publication of the person and group certificates is automated by the Persons PKI in the local directory service. User intervention is not necessary.

The publication of Commerzbank CA certificates for Commerzbank AG Inhouse Root CA, Commerzbank AG Inhouse Root CA 2 and Commerzbank AG Inhouse Sub CA 03 is executed manually on the PKI Web servers by the Crypto Services cell.

#### 4.8.7. Renewal notification of other entities by the CA

No output notification to other entities by Commerzbank CAs will take place.

### 4.9. Certificate revocation and suspension

It is primarily intended to be a certificate revocation and not a certificate suspension. Further information on certificate revocation can be obtained from the Crypto Services cell if required.

### 4.9.1. Circumstances for the block

A certificate must be revoked in the following cases:

- If the Commerzbank user Smart Card has been stolen, damaged or lost, i.e. a permanent replacement card with new certificates is issued.
- If there is a legitimate suspicion that a private key corresponding to a public key in the certificate has been compromised, i.e. that an unauthorized person can use the private key.
- If there is reasonable suspicion that the algorithms, parameters and devices used to generate and apply the private key corresponding to the public key in a signature certificate no longer guarantee the forgery security of the generated signatures.
- If the certificate holder or the certificate trustee can no longer use his certificate, e.g. the user no longer has access to the key material.
- If a certificate renewal with key change has been requested or is being requested shortly.
- When Commerzbank AG has discontinued its certification services. In this case, all certificates issued by the certification services will be revoked.
- If the certificate owner no longer fulfills the requirements for applying for the certificate, e.g. because Commerzbank employees leaves or violates the existing certificate policy.

### 4.9.2. Authorized persons to apply for a block

The following groups and instances are authorized to block certificates:

- A certificate can be revoked by
    - The certificate holder himself (certificate holder or certificate trustee),
    - His representative (by proxy),
    - His manager.
- The CA responsible for the Crypto Services cell for Commerzbank CA (Product Owner / Technical Product Manager) can initiate the blocking of CA certificates.

### 4.9.3. Perform a certificate revocation

The certificate revocation can be initiated by e-mail or by telephone. The identification (and, if necessary, authentication) of the person entitled to the application is carried out using suitable means (if necessary, from the situation).

In certain cases, the blocking is also automatic, for example, if the authorization to use the certificate is not granted when the employee leaves the company.

The certificate is generally issued by the Commerzbank RA Officer or the employees of the LRAs. For this purpose, the revocation is carried out using the certificate and smart card management system of the Persons PKI.

### 4.9.4. Notification period for revocation requests for certificate holders

There are no prescribed deadlines. As a rule, blocking entries should be reported immediately after a blocking reason has occurred.

### 4.9.5. Processing time of blocking entries by the CA

No fixed processing time of lock returns is specified by the CA.

### 4.9.6. Verification of certificate status by trusting parties

A review of certificate status by trusting parties is recommended. The lock status of Commerzbank certificates and of Commerzbank certification authorities certificates can be checked using the corresponding block lists. The current location of the certificate revocation lists can be found in the CRL Distribution Points (CDPs) contained in the certificates.

### 4.9.7. Exhibit periods for CRLs

The following issue dates and periods are valid for the PKI persons:

**Commerzbank Inhouse Root CA:**

- CRL Release Period: 4 months
- CRL Publishing Overlap Period: 1 month

**Commerzbank Inhouse Root CA 2:**

- CRL Release Period: 4 months
- CRL Publishing Overlap Period: 1 month

**Commerzbank Inhouse Sub CA 03:**

- CRL Publish Period: 1 week
- CRL Publication Overlap Period: 1 week

### 4.9.8. Maximum latency of CRLs

The CRLs are generated daily at 6:00 a.m. and made available on the Commerzbank PKI Web servers. The maximum latency is therefore 24 hours.

### 4.9.9. Online certificate revocation and status check

not applicable.

Online blocking and online status check are not intended for the Persons PKI.

### 4.9.10. Request for online check of lock status

not applicable.

An online check of the revocation status is not intended for the Persons PKI.

### 4.9.11. Other ways to promote certificate status

In addition to the announcement of Commerzbank CRLs, no other types are used on PKI Web servers.

### 4.9.12. Special measures for key compromise

If a key compromise is identified, a corresponding investigation is immediately initiated by the employees of GS-TF Cloud Foundation, cell Crypto Services. Further measures will depend on the outcome of the investigation.

#### 4.9.13. Circumstances for suspension

Not applicable, as a complete revocation of the certificate is planned.

#### 4.9.14. Eligible for suspension

Not applicable, as a complete revocation of the certificate is planned.

#### 4.9.15. Execution of a suspension

Not applicable, as a complete revocation of the certificate is planned.

#### 4.9.16. Duration of suspension

Not applicable, as a complete revocation of the certificate is planned.

### 4.10. Certificate Status Information Services

Commerzbank AG operates an information service based on certificate revocation lists (CRLs) about the certificate status. This information service is web-based and is provided by the URL

http://ca.commerzbank.com/cdp/

The CRLs are published:

- The status information for the person and group certificates is published in the CRL by Commerzbank AG Inhouse Sub CA 03. Due to a key renewal, two revocation lists are currently being provided.
- The status information for the certificates of the certification authorities is published in the CRLs by Commerzbank AG Inhouse Root CA or Commerzbank AG Inhouse Root CA 2.

Separate CRLs (revocation lists) are published for each of these certificate types.

#### 4.10.1. Operational characteristics

The directory service is web-based and uses http as the transfer protocol.

The CRLs of the Root CA, Root CA 2, or Sub CA 03 can be obtained from the following URLs:

- Certificate revocation list Commerzbank AG Inhouse Root CA
  http://ca.commerzbank.com/cdp/coba_root.crl
- Certificate revocation list Commerzbank AG Inhouse Root CA 2
  http://ca.commerzbank.com/cdp/coba_rootca2.crl
- Certificate revocation list Commerzbank AG Inhouse Sub CA 03
  *In-house Sub CA 03 (old):* http://ca.commerzbank.com/cdp/coba_sub03(1).crl

  *In-house Sub CA 03:* http://ca.commerzbank.com/cdp/coba_sub03(2).crl

The CRLs and certificates to be revoked must have been issued by the same CA. There is no support for "indirect CRLs" in the current implementation.

The CRL profile issued is compliant with RFC 5280 and complies with the X.509 version 2 standard.

#### 4.10.2. Availability of the information service

The availability of the Commerzbank PKI Web server is designed for 7x24 operation.

#### 4.10.3. Optional features

Optional features are not provided.

## 4.11. Termination of the contractual relationship by the certificate holder

A certificate holder or certificate trustee of a Commerzbank certificate will be excluded from the certification services if he leaves Commerzbank AG's employment or if his employment as an external employee ends. This end of the contract will void the Certificate Usage privilege and will automatically lock the certificate.

## 4.12. Key deposit and recovery

Key deposit and recovery are practiced within the scope of the Persons PKI for encryption keys.

A backup copy of the keys is used to restore user keys. The implementation is carried out by the Smart Card Management System and the certificate management system of the certification authority Commerzbank AG Inhouse Sub CA 03, which archives the key material of the user encrypted in the CA database.

A detailed description of this process can be obtained from the Crypto Services cell.

#### 4.12.1. Key deposit and key recovery policies and practices

A recovery guideline was developed within the framework of Commerzbank Persons PKI.

A detailed description of this process can be obtained from the Crypto Services cell.

#### 4.12.2. Policies and practices for the deposit and recovery of session keys (Symmetric keys)

Not applicable. Session keys are not archived.

# 5. Facilities, security management, organizational and operational security measures

## 5.1. Physical and environmental security

The infrastructure security measures of Commerzbank Persons PKI are embedded in Commerzbank AG data center operations. The following precautions and physical protection measures are an integral part of the data centers operated by Commerzbank AG.

### 5.1.1. Location and construction

Commerzbank Persons PKI systems are located in the Commerzbank data centers. The rooms provide adequate protection with regard to physical safety measures, which is adequate to the required level of safety.

### 5.1.2. Access control

The premises of the certification authorities are protected by appropriate technical and infrastructural measures. Access to the certification authority's premises is only permitted to employees who have the appropriate approval level. Access by non-operating persons is defined by a visitor regulation.

### 5.1.3. Power supply and air conditioning

The installation for the power supply complies with the required standards, air conditioning of the rooms for the technical infrastructure is available.

### 5.1.4. Water damage

The technical infrastructure rooms have adequate protection against water damage.

### 5.1.5. Prevention and protection against fire

The existing fire protection regulations are complied with.

### 5.1.6. Media

The following disks are used:

- Paper
- CD-ROMs
- USB memory modules
- Hardware tokens

Disks are stored in locked cabinets. Data media with sensitive data, such as HSM hardware tokens, stored in a vault.

### 5.1.7. Waste Disposal

Information on electronic data carriers is properly destroyed and then disposed of appropriately. Paper data media are destroyed by means of existing shredders and disposed of properly here as well.

### 5.1.8. Off-site backup

Commerzbank data center operations regulate the creation of off-site backups.

## 5.2. Organizational security controls

### 5.2.1. Safety-critical roles

Security-critical tasks are summarized in roles for the operation of Commerzbank Persons PKI. A PKI role concept is available and is implemented for the organizational process and also for HSM (Hardware Security Module) operation.

A description of the role definition can be obtained from the Crypto Services cell if required.

### 5.2.2. Assigned number of people for safety-critical tasks

The four-eye principle applies to the following operations:

- Restoring the key material of Commerzbank certification authorities
- Restoring Commerzbank certification authorities
- (Administrative) access to the hardware security modules of the Commerzbank certification authorities

### 5.2.3. Identification and authentication of roles

Users are identified and authenticated when accessing security-related rooms and when accessing security-related systems using smart cards, hardware tokens and/or usernames and passwords.

For particularly security-critical operations, such as the management of CA keys, the four-eyes principle is implemented.

### 5.2.4. Separation of roles and tasks

The role concept also regulates which assignments of persons to roles are mutually exclusive.

Detailed information on role and task separation can be obtained from the Crypto Services cell.

## 5.3. Personnel security measures

Commerzbank AG provides experienced personnel within the scope of the Persons PKI. The necessary qualification, knowledge and experience of the personnel are available for secure PKI standard operation.

### 5.3.1. Requirement for qualification, experience and approval level

The responsible personnel have the necessary specific knowledge and experience in the area of Persons PKI. Basic IT skills are also available to perform system-related operations.

### 5.3.2. Employee Security Review Process

The general personnel recruitment guidelines of Commerzbank AG also apply. The employees used in the context of the PKI are subjected to special security checks (e.g. checking of the leadership certificate).

### 5.3.3. Training request

The personnel assigned to the certification service will be adequately trained before starting the work. The training also includes raising awareness among employees about the security relevance of their work and potential threats.

### 5.3.4. Training frequency

The frequency of the training sessions is based on the requirements of Commerzbank Persons PKI. Training sessions are held in particular when new policies, IT systems and security technology are introduced.

### 5.3.5. Frequency and sequence of job rotation

A job rotation is not planned.

### 5.3.6. Sanctions for prohibited actions

Commerzbank AG's general sanctions are applied in the event of inadmissible actions.

### 5.3.7. Terms and conditions for personnel

Commerzbank PKI operating personnel are obliged to comply with instructions and legal regulations. These include in particular an obligation to treat personal data confidentially in accordance with the European General Data Protection Regulation (EU-GDPR).

### 5.3.8. Documents handed out to staff

The following documents are provided to the PKI operating personnel for the proper operation of the Persons PKI:

- Certificate Policy (CP)
- Certification Operations or Certification Practice Statement (CPS)
- Operating concept and security concept of the Persons PKI
- Instructions for action
- Operating manuals for systems and software

## 5.4. Monitoring of safety-critical events

### 5.4.1. Logged events

The following data is collected for each event:

- Time (date and time)
- Log ID of the entry
- Type of event
- Origin of the event

### 5.4.2. Check frequency of log data

Log data should be reviewed at regular intervals. If irregularities are suspected, an immediate check is initiated.

### 5.4.3. Retention periods for audit log data

Security-relevant log data is retained in accordance with the regulations of Commerzbank AG.

### 5.4.4. Protection measures for audit log data

Electronic log files are protected against access, deletion and manipulation by means of the operating system and are only accessible to system and network administrators.

### 5.4.5. Audit log data backup procedures

The log data is backed up regularly with other relevant data. Paper logs are stored in lockable cabinets.

### 5.4.6. Audit Collection System (Logging System)

All log files are backed up regularly in the sense of a backup.

### 5.4.7. Notification when a safety-critical event is triggered

Notification of the PKI operator personnel occurs in the event of production problems.

### 5.4.8. Vulnerability analysis

A vulnerability scan is performed on a monthly basis for the CA servers.

## 5.5. Archive log data

Commerzbank AG archives protocol data defined as part of the PKI operation.

### 5.5.1. Archived log data types

Log data relevant to the certification process is archived:

- Certificate requests, which contain the personal data of the certificate holder
- All certificates issued by the CA
- Revocation requests for certificates and for certification authority certificates
- System data backed up before a modification of a system
- Backups of the productive systems
- Documentation of personnel security measures (e.g. schedules, documentation of safety checks)
- Documentation of procedures and systems (e.g. operating instructions, emergency plans, system manuals)
- Protocols of security-related internal procedures and processes

### 5.5.2. Archiving deadlines

Data to be archived is retained in accordance with Commerzbank regulations.

### 5.5.3. Protection measures for the archive

Appropriate measures are taken to ensure that the data cannot be changed or deleted. If personal data is contained in the archives, it is also ensured that the data cannot be read or copied without authorization.

The protective measures for electronic data carriers correspond to the processes planned for the data center operation of Commerzbank AG.

### 5.5.4. Backup procedures for the archive

The procedures and processes for archive backup follow the implementation planned for the Commerzbank AG data center operations.

### 5.5.5. Timestamp requests for archived data

Audit logs, logged events, archived data, certificates, certificate revocation lists, and other entries each contain a unique time and date. Online system dates and times are synchronized at regular intervals against a trustworthy time source.

### 5.5.6. Archiving system (internal or external)

An archiving system is used within the framework of Commerzbank Persons PKI.

### 5.5.7. Procedures for obtaining and verifying archive data

The Commerzbank Persons PKI operating concept describes the processes for requesting and verifying archive data.

A detailed description of this process can be obtained from the Crypto Services cell.

## 5.6. Key changes of the certification authorities

When Commerzbank AG Inhouse Root CA changes keys, the private key corresponding to the old CA certificate is destroyed and a new self-signed certificate issued and published. The name of the new CA certificate reflects the change by adding or incrementing an index. The root CA certificate currently in use is Commerzbank AG Inhouse Root CA 2. The self-signed root CA certificates cannot be blocked technically on the CA side.

When Commerzbank AG Inhouse Sub CA 03 changes its key, a new key pair is generated and a new certificate issued and published. Certificates are then issued via the new keys. CRL and certificate of the previous Sub CA 03 keys will continue to be provided as long as valid certificates created by the respective Sub CA 03 exist and the Sub CA 03 certificate has not been revoked for other reasons. The application itself is made by Commerzbank AG Inhouse Sub CA 03.

The CA certificate renewal with key change follows the schema listed below:

**Commerzbank AG Inhouse Root CA / Commerzbank AG Inhouse Root 2**

- Root CA certificate: 30 years
- Root CA CRLs: 4 months
- Renewal period Commerzbank AG Inhouse Root CA / Commerzbank AG Inhouse Root CA 2 certificate no later than 12 months prior to expiration

**Commerzbank AG Inhouse Sub CA 03**

- Sub CA 03 certificate: 7 years
- Sub CA 03 CRLs: 14 days
- Renewal period Commerzbank AG Inhouse Sub CA 03 certificate no later than 6 months before expiration

## 5.7. Compromise and restart after disasters

### 5.7.1. Procedures for security incidents and compromise

There are emergency plans of Commerzbank AG, in which the processes, procedures and responsibilities in the event of emergencies and disasters are regulated. The objective of these emergency procedures is to minimize the failure of certification services while maintaining security. Emergency procedures specifically provide for the following measures in the event of a security incident:

- Analyze and evaluate the functional limitations and security issues of the affected services and certification authority systems
- Establish immediate actions to address functional limitations and security issues
- Control of responsibilities and roles
- If necessary, notification of affected authorities and persons, e.g. the certificate holder, about the problem and, if necessary, necessary countermeasures
- Analysis and documentation of the causes of the incident
- If necessary, create, review, and approve a change request to modify the system configuration to prevent future incidents of this type. Monitoring the implementation of the change request
- Logging of the individual measures and activities

### 5.7.2. Compromise of IT resources

If the CA detects faulty or compromised machines, software, and/or data that affects the CA's processes,

- the operation of the corresponding IT system is stopped immediately.
- the IT system is restarted by restoring the software and data from the data backup, checking and commissioning in a safe state.
- the faulty or modified IT system is then analyzed. If a deliberate act is suspected, legal action may be taken.
- the certificate holder is informed immediately, if his certificate contains incorrect information, and the certificate is revoked.

### 5.7.3. Restart if private key material is compromised

The compromise of private key material is a serious incident and is therefore handled in a special way.

- If private key material from the certification authorities is compromised, the respective certificate is immediately blocked. At the same time, all certificates issued with this certificate are revoked.
- If private key material of Commerzbank user certificate for Smart Cards and certificates for group mailboxes is compromised, the respective certificate is immediately revoked.
- If it is suspected that the algorithms, parameters or devices used to generate and use the private key are unsafe, an appropriate investigation will be conducted.
- All affected certificate holders and trusting parties will be notified immediately.

### 5.7.4. Emergency operation after a disaster

A resumption of certification operations after a disaster is part of the emergency planning and can take place within a short time, provided that the safety of the certification service is ensured.

### 5.7.5. Termination of the operation of the certification and/or registration authority

The following measures are defined in the event that Commerzbank AG certification authorities or registration authorities stop operating:

- All certificate holders and trusting parties will be informed of the termination of the certification service. A time limit has not yet been set.
- All user certificates, as well as the certificates of the certification authorities, are blocked.
- All certificate authority private keys and user certificates for smart cards of the certificate holders are destroyed.
- The key material for encryption is the exception. These are archived in secure environments, such as an encrypted database.

# 6. Technical safety measures

## 6.1. Key pair generation and installation

### 6.1.1. Key pair generation

The key generation and selection of the crypto algorithms for Commerzbank Persons PKI is carried out in accordance with Commerzbank specifications and according to FIPS 140-2 level 1 and 3 (Federal Information Processing Standards).

The generation of key pairs is performed by hardware and software components and differs according to the entity:

*Key pair generation for Commerzbank certification authorities:*

All key pairs for Commerzbank certification authorities are generated by the Network Hardware Security Module (HSM). The generated CA keys are also cryptographically protected by the HSM network. Any process that requires access to the CA's private key is mandatory for the HSM. Commerzbank Network HSM operates in FIPS 140-2 Level 3 mode.

*Key Pair Generation for Commerzbank Group Certificates:*

The key pairs for group certificates are generated by the Persons PKI on the computer of the certificate trustee. In this case, the key material is generated by software components. The Crypto components are FIPS 140-2 Level 1 certified.

*Key pair generation of keys for Commerzbank user certificates on Smart Cards:*

The authentication and signature key pairs for the person certificates are generated by the certificate holder's smart card used. In this case, the key material is generated by hardware. The hardware crypto components on the Smart Card are FIPS 140-2 Level 3 certified.

In contrast, the generation of the person encryption key pair by the certificate management system takes place in the HSM of the PKI. This allows encryption keys to be archived. Commerzbank Network HSM operates in FIPS 140-2 Level 3 mode.

### 6.1.2. Delivery of the private keys to the certificate holder

*Private keys of Commerzbank certification authorities:*

Any process that requires access to the CA's private key is mandatory for the HSM; all private CA keys are only available in the HSM itself.

It is not necessary to deliver CA keys private key material, as the HSM is used for key generation and as a secure storage for private keys. Backup tokens are used to store the private key material on the HSM.

*Private keys for Commerzbank user certificates on Smart Cards*

The certificate holder is provided with a Smart Card as the medium for private keys and the associated certificates. The Smart Card is delivered without key pairs and certificates. As part of Smart Card provisioning, the key pairs for person certificates are generated on the used Smart Card, or subsequently applied in the case of encryption keys.

Access to the private key is only granted after successful activation by a user PIN.

*Private keys of Commerzbank group certificates:*

The key pairs are generated on the requesting machines themselves.

Subsequent manual delivery is not necessary. In this case, the delivery of the private key to the application machine is automated via suitable secure procedures, such as downloading a PKCS#12 file.

### 6.1.3. Delivery of the public keys to certificate issuers

The certificate signing request (CSR) of the certificate holder or certificate trustee is sent by the Persons PKI to the certification authority for the purpose of certification in PKCS#10 format. The entire process is automated.

The certificate signing request from Commerzbank AG Inhouse Sub CA 03 is also in PKCS#10 format. However, due to the offline facial expressions of Commerzbank AG Inhouse Root CA, this process takes place purely manually.

### 6.1.4. Delivery of public CA keys to confidential parties

The public CA keys are delivered manually. In addition, the public keys of the Commerzbank certification authorities are published on the web URLs provided for this purpose:

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

*Commerzbank AG Inhouse Root CA 2:* http://ca.commerzbank.com/aia/coba_rootca2.crt

*Commerzbank AG Inhouse Sub CA 03:* http://ca.commerzbank.com/aia/coba_sub03(2).crt

Until September 2020:

*Commerzbank AG Inhouse Sub CA 03 (old):* http://ca.commerzbank.com/aia/coba_sub03(1).crt

### 6.1.5. Key lengths

According to Commerzbank AG specifications, the Coba PKI and the Persons PKI were parameterized as follows:

*Commerzbank CA Key Length:*

- Commerzbank AG Inhouse Root CA - 4096bit (HSM) - RSA Algorithm
- Commerzbank AG Inhouse Root CA 2 – 4096bit (HSM) – RSA algorithm
- Commerzbank AG Inhouse Sub CA 03 – 4096bit (HSM) – RSA algorithm
- Commerzbank AG Inhouse Sub CA 03 (until September 2020) - 2048bit (HSM) - RSA algorithm

*Commerzbank Certificate holder Key length:*

- Commerzbank Smart Card User Certificates - 2048bit - RSA Algorithm
- Commerzbank Group Mailbox Certificates - 2048bit - RSA Algorithm

### 6.1.6. Generation and verification of key parameters

The following OIDs are used:

- Public Key Algorithm: 1.2.840.113549.1.1.1 (RSA)
- Signature algorithm: 2.16.840.1.101.3.4.2.1 (sha256RSA)
- Signature algorithm (stock certificates issued until September 2020): 1.2.840.113549.1.1.5 (sha1RSA)

### 6.1.7. Key use purpose (key usage field according to X.509 version 3)

See also Section 7.1 Certificate and CRL Profiles

*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 Root CA 2 - 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 Certificate holder Key use:*

- Commerzbank Group mailboxes - 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 modules

Private keys in Commerzbank Persons PKI are protected by cryptographic modules in the form of hardware or software.

Protecting the private keys of:

- Commerzbank certification authorities are covered by the Hardware Security Module
- Commerzbank personal certificates are issued by a hardware implementation of the Crypto interface Smart Cards and
- Commerzbank group certificates for group mailboxes are implemented by a software implementation of the Crypto interface

### 6.2.1. Standards and security measures of cryptographic modules

- The HSM network used has been evaluated according to FIPS 140, Level 2 and Level 3.
- The used smart cards are evaluated according to FIPS 140 level 3.
- The software Crypto modules used have been evaluated according to FIPS 140 level 1.

### 6.2.2. More personal control of private keys (n of m procedure)

Private key sharing does not occur. The operation of the HSM network is an exception. An n-of-m procedure for network HSM management has been set up.

### 6.2.3. Private key deposit

The private keys of the Commerzbank certification authorities are deposited using HSM backup tokens.

### 6.2.4. Backup of private keys

Private key material from Commerzbank certification authorities is secured by the HSM network and associated HSM backup tokens and processes.

Private key material of Commerzbank Certificate holders and certificate holders for encryption keys are secured by the Persons PKI offered backup mechanisms.

A detailed description of the two processes mentioned above can be obtained from the Crypto Services cell.

### 6.2.5. Archiving private keys

Private keys are only archived for encryption keys. A backup/archive key is available to restore private key material.

Detailed information can be obtained from the Crypto Services cell.

### 6.2.6. Transfer of private keys to or from a cryptographic module

Private key transfers are for encryption keys only. To do this, the key material is generated outside the cryptographic module (Smart Cards) and imported downstream into the cryptographic module (Smart Card). This procedure is necessary to archive encryption key material.

Private key material from Commerzbank certification authorities is backed up by the HSM network's own backup components (backup tokens) and processes.

### 6.2.7. Storage of private keys in the cryptographic module

The private keys of Commerzbank AG Inhouse Root CA, Commerzbank AG Inhouse Root CA 2 and Commerzbank AG Inhouse Sub CA 03 are managed and protected by the HSM network. In addition, a backup of the CA keys is performed by the HSM network, which in turn are stored in a physically protected environment. The HSM network is FIPS 140 Level 3 certified.

The private keys for user certificates on Smart Cards are protected by the inserted Smart Card and stored in a secure area on the Smart Card. The Smart Cards used are FIPS 140 Level 3 certified.

The private keys for Commerzbank Group mailbox are managed and stored securely on the requesting machine by a software crypto component. The Crypto components are FIPS 140-2 Level 1 certified.

### 6.2.8. Private key activation

Private key activation is only for Smart Card-based keys. Activation and thus access to the private key is done by setting a Smart Card PIN by the user.

### 6.2.9. Private key deactivation

Not applicable. Private key deactivation is not intended for Commerzbank Persons PKI. For this reason, testing CRLs in applications is critical.

### 6.2.10. Destruction of private keys

The methods of destroying private keys by the certification service provider depend on the cryptographic hardware and/or software in which the keys are stored:

- The destruction of all private key material is usually done by deleting the private key store. Individual deletion of private keys must be implemented manually.
- Private CA keys stored in HSMS are destroyed by deleting the key in the HSM.
- Private keys present on smart cards are deleted by initialization or formatting.

### 6.2.11. Evaluation of the cryptographic module

- The HSM network used is operated according to FIPS 140 level 3.
- The smart cards used are operated in accordance with FIPS 140 level 3.
- The software crypto modules used are operated according to FIPS 140 level 1.

## 6.3. Other aspects of managing key pairs

### 6.3.1. Archiving of public keys

All certificates issued by the Certification Services are archived in the Certification Authority database. In addition, there is no archiving of public keys.

### 6.3.2. Validity of certificates and key pairs.

The following life periods have been defined for Commerzbank AG certification authorities:

**Commerzbank AG Inhouse Root CA**

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

**Commerzbank AG Inhouse Root CA 2**

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

**Commerzbank AG certificates for smart cards**

- Commerzbank Smart Card Certificates: 3 years
- Certificate renewal with key change

**Commerzbank AG Certificates for group mailboxes**

- Commerzbank Group mailbox Certificate: 3 years
- Certificate renewal with key change

## 6.4. Activation data

Activation data that controls access to Smart Card-based private keys is generated by Commerzbank Persons PKI.

Activation data is generated when smart cards are issued in the form of PIN and PUK for Commerzbank users.

### 6.4.1. Creation of activation data and installation

The randomly generated activation data (PUK) is generated by the certificate and smart card management system.

### 6.4.2. Protection of activation data

The activation data (PIN and PUK) is protected by the certificate and smart card management system. To do this, this data is stored encrypted on the associated certificate management database. Access to this is exclusive to the management system only.

### 6.4.3. Other aspects of activation data

Not applicable.

## 6.5. Security measures for computers

### 6.5.1. Specific technical requirements of computer security measures

Servers that implement core functionality of the certification services and any machines that protect the certification services facilities are subject to the following security requirements:

- Only the software required for the respective function is installed on the server.
- The server only has the communication interfaces required for the respective function. In particular, the computers are only integrated into the networks required for their function.
- Unnecessary functions of the operating system and the installed software are deactivated, if possible.
- If security risks become known in the software being used, system administrators will promptly take the countermeasures recommended by the manufacturer or independent experts. In particular, the operating system and the software are always updated with the latest patches against known security vulnerabilities.
- Access to the servers is limited to what is necessary to operate the certification services. In particular, the servers are only managed by the responsible system administrators.
- Security-critical events on the computers are logged.
- Systems with high availability requirements are designed to be highly available, so that the function is retained in the event of a computer failure.

- By means of uninterruptible power supplies and by means of aggregates, fluctuations in the power supply are compensated and power failures are bridged up to a duration of several hours.
- Only scanned media (virus, malware protection) may be used on the systems.

### 6.5.2. Evaluate computer security

Commerzbank Persons PKI is based on certification services that are evaluated according to Common Criteria EAL (Evaluation Assurance Level) 4+ (FLR – augmented with Flow Remediation).

The HSM network used has been evaluated according to FIPS 140, Level 2 and Level 3.

The used smart cards are evaluated according to FIPS 140 level 3.

The software crypto modules used have been evaluated according to FIPS 140 level 1.

## 6.6. Technical controls for the entire life cycle

### 6.6.1. Security measures for system development

Not applicable.

There is no system development.

### 6.6.2. Security management

The Persons PKI are subject to Commerzbank's standard security processes and security management.

### 6.6.3. Security measures for the entire lifecycle

Within the framework of the security concept for Commerzbank Persons PKI and the associated certification authorities, the necessary security measures are examined.

If required, detailed information about the security concept can be obtained from the Crypto Services cell.

## 6.7. Safety measures in the network

The certification services implement the following network security measures:

- The productive systems and networks are separated from the Internet by firewalls.
- The internal networks of the certification services are divided as far as possible according to the protection requirements of the systems. The separation into subnets is done by firewalls.
- Firewalls restrict traffic to what is necessary for operation.
- Communication between the switches is encrypted.

## 6.8. Time stamp

Commerzbank certification authorities use time stamps when issuing certificates and certificate revocation lists. The time source used here is the local system clock of the computer system used. The local system clock of the online servers (the AD-Member Server) is synchronized regularly with an external time source (the AD controllers). The offline instances of Commerzbank Inhouse Root CA receive their time setting via the hypervisor (VMware).

The use of an additional trusted and evaluated timestamp component is not necessary for the Persons PKI solution.

# 7. Certificate and CRL profile

Within the scope of the PKI persons, certificate and CRL profiles are defined for the relevant Commerzbank AG CA instances. These profiles follow the PKIX requirements according to RFC 5280 and focus in particular on the interoperability aspects.

Extensions for the certificate and CRL profiles are provided, so far as they can be used for the purpose of distinguishing certificate types.

## 7.1. Certificate Profile

Commerzbank certificates correspond to:

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

Commerzbank certificate profiles are compliant:

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

The basic description of Commerzbank certificates contains:

| **Field** | **Value** |
|---|---|
| Version | See also *7.1.1. Version Numbers(s)* |
| Serial number | Unique value in the namespace of each CA |
| Signature Algorithm | Designation of algorithm used to sign the certificate. See also *7.1.3. Algorithm Object Identifiers* |
| Issuer | see also *7.1.4. Name Forms* |
| Validity | Validity (from and to) time and date information. |
| Subject | see also *7.1.4. Name Forms* |
| Subject Public Key | Public Key Blob |
| Signature | CA signature |

### Commerzbank AG CA Certificates:

| **Commerzbank AG Inhouse Root CA 2** | |
|---|---|
| X.509 version | V3 |
| Serial number | 70 31 45 df 1b 51 d1 b0 48 67 92 8f 1d 3d 52 38 |
| Signature Algorithm | sha256RSA |
| Signature Hash Algorithm | sha256 |
| Issuer | CN = Commerzbank AG Inhouse Root CA 2<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |

| | |
|---|---|
| Key Length | 4096 |
| Valid from | Tuesday, September 29, 2015 12:07:26 |
| Valid to | Friday, September 29, 2045 12:17:21 |
| Public key | RSA (4096-bit) Key Blob |
| Subject | CN = Commerzbank AG Inhouse Root CA 2<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Usage | Digital Signature, Certificate Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline) |
| Subject Key Identifier | 82 11 39 57 df ff 92 ff d3 74 78 52 b9 f8 9b 14 e7 c8 bd 34 |
| 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 | 62 00 00 00 0d ba a0 d7 fc 98 2f e2 80 00 00 00 00 00 0d |
| Signature Algorithm | sha256RSA |
| Signature Hash Algorithm | sha256 |
| Issuer | CN = Commerzbank AG Inhouse Root CA 2<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Length | 4096 |
| Valid from | Tuesday, September 15, 2020 07:52:47 |
| Valid to | Wednesday, September 15, 2027 08:02:47 |
| Public key | RSA (4096-bit) Key Blob |
| Subject | CN = Commerzbank AG Inhouse Sub CA 03<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Usage | Digital signature, certificate signature, offline signing of the CRL, signing the CRL (86) |
| Subject Key Identifier | 47 ec b0 33 2e 1a 73 b9 f6 42 2e c5 00 09 73 1f c8 b4 76 f4 |

| | |
|---|---|
| Authority Key Identifier | 82 11 39 57 df ff 92 ff d3 74 78 52 b9 f8 9b 14 e7 c8 bd 34 |
| CRL Distribution Points | http://ca.commerzbank.com/cdp/coba_rootca2.crl |
| Authority Information Access | http://ca.commerzbank.com/aia/coba_rootca2.crt |
| Subject Alternative Name | None |
| Extended Key Usage | None |
| Thumbprint Algorithm | sha1 |
| Thumbprint | 3d 31 76 29 5e 25 03 75 07 51 fa e9 c0 37 8c 1c 4e f5 90 35 |

For stock certificates only (issued until September 2020):

| **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<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Length | 4096 |
| Valid from | Wednesday, December 7, 2005 14:15:17 |
| Valid to | Friday, December 7, 2035 14:16:04 |
| Public key | RSA (4096-bit) Key Blob |
| Subject | CN = Commerzbank AG Inhouse Root CA<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>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 approx. 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 (until September 2020) | |
|---|---|
| X.509 version | V3 |
| Serial number | 61 13 b7 9b 00 00 00 00 00 0c |
| Signature Algorithm | sha1RSA |
| Issuer | CN = Commerzbank AG Inhouse Root CA<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Length | 2048 |
| Valid from | Monday, May 9, 2016 09:11:18 |
| Valid to | Tuesday, 9. May 2023 09:21:18 |
| Public key | RSA (2048-bit) Key Blob |
| Subject | CN = Commerzbank AG Inhouse Sub CA 03<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Usage | Digital signature, certificate signature, offline signing of the CRL, signing the CRL (86) |
| Subject Key Identifier | af ff f0 ee f9 c7 a6 fe b7 02 ac 80 5e ce fa b6 87 dd 6d 5d |
| Authority Key Identifier | 8c f9 89 bf 7e 3c approx. 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 | ec bf b1 df 12 a7 79 1a be b7 13 46 39 e2 ad b8 65 66 03 db |

## Commerzbank AG Smart Card Certificates:

| Coba SC Authentication | |
|---|---|
| X.509 version | V3 |
| Serial number | [Certificate Serial Number] |
| Signature Algorithm | sha256RSA |
| Issuer | CN = Commerzbank AG Inhouse Sub CA 03<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>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><br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Usage | Digital Signature |
| Subject Key Identifier | [corresponding private key] |
| Authority Key Identifier | 47 ec b0 33 2e 1a 73 b9 f6 42 2e c5 00 09 73 1f c8 b4 76 f4 |
| CRL Distribution Points | http://ca.commerzbank.com/cdp/coba_sub03(2).crl |
| Authority Information Access | http://ca.commerzbank.com/aia/coba_sub03(2).crt |
| Subject Alternative Name | <User Principal Name> |
| Extended Key Usage | Smart Card Enrollment (1.3.6.1.4.1.311.20.2.2)<br>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 | sha256RSA |
| Issuer | CN = Commerzbank AG Inhouse Sub CA 03<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>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 = <email address><br>CN = <last name>, <first name><br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Usage | Digital Signature, Non Repudiation |
| Subject Key Identifier | [corresponding private key] |

| | |
|---|---|
| Authority Key Identifier | 47 ec b0 33 2e 1a 73 b9 f6 42 2e c5 00 09 73 1f c8 b4 76 f4 |
| CRL Distribution Points | http://ca.commerzbank.com/cdp/coba_sub03(2).crl |
| Authority Information Access | http://ca.commerzbank.com/aia/coba_sub03(2).crt |
| Subject Alternative Name | <RFC 822 email address> |
| Extended Key Usage | Secure email (1.3.6.1.5.5.7.3.4)<br>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 | sha256RSA |
| Issuer | CN = Commerzbank AG Inhouse Sub CA 03<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>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 = <email address><br>CN = <last name>, <first name><br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Usage | Key Encipherment |
| Subject Key Identifier | [corresponding private key] |
| Authority Key Identifier | 47 ec b0 33 2e 1a 73 b9 f6 42 2e c5 00 09 73 1f c8 b4 76 f4 |
| CRL Distribution Points | http://ca.commerzbank.com/cdp/coba_sub03(2).crl |
| Authority Information Access | http://ca.commerzbank.com/aia/coba_sub03(2).crt |
| Subject Alternative Name | <RFC 822 email address> |
| Extended Key Usage | BitLocker Drive Encryption (1.3.6.1.4.1.311.67.1.1)<br>Secure email (1.3.6.1.5.5.7.3.4)<br>Encrypting File System (1.3.6.1.4.1.311.10.3.4) |
| Thumbprint Algorithm | sha1 |
| Thumbprint | [Thumbprint of certificate] |

Commerzbank AG Certificates for Group mailboxes:

| Commerzbank Soft PSE Encryption | |
|---|---|
| X.509 version | V3 |
| Serial number | [Certificate Serial Number] |
| Signature Algorithm | sha256RSA |
| Issuer | CN = Commerzbank AG Inhouse Sub CA 03<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>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 = <email address Group mailbox><br>CN = <group mailbox name><br>OU = Team mailbox<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| Key Usage | Key Encipherment |
| Subject Key Identifier | [corresponding private key] |
| Authority Key Identifier | 47 ec b0 33 2e 1a 73 b9 f6 42 2e c5 00 09 73 1f c8 b4 76 f4 |
| CRL Distribution Points | http://ca.commerzbank.com/cdp/coba_sub03(2).crl |
| Authority Information Access | http://ca.commerzbank.com/aia/coba_sub03(2).crt |
| Subject Alternative Name | <RFC 822 email address Group mailbox> |
| Extended Key Usage | Secure email (1.3.6.1.5.5.7.3.4) |
| Thumbprint Algorithm | sha1 |
| Thumbprint | [Thumbprint of certificate] |

For stock certificates only (issued until September 2020):

The certificate profiles correspond to the profiles described above with the following deviations:

| | |
|---|---|
| Signature Algorithm | sha1RSA |
| Authority Key Identifier | af ff f0 ee f9 c7 a6 fe b7 02 ac 80 5e ce fa b6 87 dd 6d 5d |
| CRL Distribution Points | http://ca.commerzbank.com/cdp/coba_sub03(1).crl |
| Authority Information Access | http://ca.commerzbank.com/aia/coba_sub03(1).crt |

### 7.1.1. Version Number(s)

Commerzbank AG Inhouse Root CA 2 and Commerzbank AG Inhouse Sub CA 03 issue X.509 version 3 certificates.

### 7.1.2. Certificate Extensions

The following certificate extensions are included in the certificates provided by Commerzbank:

| Enlargement | Value | Critical |
|---|---|---|
| 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 corresponds 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 observed. | No |
| Authority Information Access | Contains a link where additional information to the issuing CA can be observed (ca issues method). | No |
| Extended Key Usage | Contains application specific attributes/OIDs. | No |
| Subject Alternative Name | Contains alternative subject names, such as e-mail address or UPN. | No |
| Certificate Issuance Policies | 1.3.6.1.4.1.14978.5.1 (Commerzbank AG CP/CPS OID Reference) | No |

The following private certificate extensions apply:

| Enlargement | 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

- The Commerzbank certification authorities create RSA key pairs (OID: 1.2.840.113549.1.1.1) in accordance with RFC 5280.
- The Commerzbank certification authorities create signatures with shab265WithRSAEncryption
  (OID : 2.16.80.1.101.3.4.2.1) per RFC 5280.

### 7.1.4. Name Forms

The CA certificates issued by **Commerzbank AG Inhouse Root CA (Root CA and Root CA 2)** contain the complete Distinguished Name (DN) in the Subject Name and Issuer Name fields.

The DN is structured in accordance with X.500 and contains the components in the following order:

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

The **end entities certificates** issued by **Commerzbank AG Inhouse Sub CA 03**, i.e. person certificates and group certificates contain the complete distinguished name (DN) in the subject name and in the issuer name field. The DN is structured in accordance with X.500 and contains the components in the following order:

**The certificate type Coba SC Authentication** is:

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

**The following** applies to the certificate type Coba SC Signature, Coba SC Encryption:

E = [RFC 822 email Address],
CN = [Common Name],
O = [Organization],
L = [Locality],
C = [Country]

The certificate type **Commerzbank Soft PSE Encryption** is:

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 restrictions related to names.

### 7.1.6. Certificate Policy Object Identifier

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

### 7.1.7. 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 provided by a URL:

- http://ca.commerzbank.com/cpcps.en.html

### 7.1.9. Processing Semantics for Critical Certificate Policies Extension

not applicable.

## 7.2. CRL Profile

CRLs are issued as part of Commerzbank Persons PKI. It is not planned to issue "delta CRLs" in the case of Commerzbank Root CA or Root CA 2.

Commerzbank CRL profiles correspond to:

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

Commerzbank CRL profiles are compliant:

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

The base CRL fields are defined as follows:

| **Field** | **Value** |
|---|---|
| Version | See also *7.2.1. Version Number* |
| Issuer | Contains the DN 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.<br>See also *7.1.3. Algorithm Object Identifiers* |
| Signature | CA signature |

| **Commerzbank AG Inhouse Root CA 2 - CRL Profile** | |
|---|---|
| **Field** | **Value** |
| Version | X.509 V2 |
| Issuer | CN = Commerzbank AG Inhouse Root CA 2<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |

| | |
|---|---|
| This update / Valid from | [Time and date of CRL issuance] |
| Next update | [Time and date of next CRL update] |
| Signature Algorithm | sha256RSA |
| **Extension** | **Value** |
| Authority Key Identifier | 82 11 39 57 df ff 92 ff d3 74 78 52 b9 f8 9b 14 e7 c8 bd 34 |
| CRL Number | [Unique Increasing Number per CRL] |
| Approx. Version | Starting from: V0.0 |
| Next CRL Publish | [Time and date of next CRL publish] |
| **Reverted Certificates** | **Value** |
| Certificate Serial Number | [Serial Number of reverted Certificate] |
| Revocation Date | [Time and date of Certificate revocation] |
| Reason code | Revocation Reason:<br>unspecified, keyCompromise, cACompromise, affiliate Changed, superseeded, cessationOfOperation, certificateHold, removeFromCRL |

| **Commerzbank AG Inhouse Root CA - CRL Profile** | |
|---|---|
| **Field** | **Value** |
| Version | X.509 V2 |
| Issuer | CN = Commerzbank AG Inhouse Root CA<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>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 approx. 24 31 cc 70 c6 95 9d 72 47 36 27 c8 67 |
| CRL Number | [Unique Increasing Number per CRL] |
| Approx. Version | Starting from: V0.0 |
| Next CRL Publish | [Time and date of next CRL publish] |
| **Reverted Certificates** | **Value** |
| Certificate Serial Number | [Serial Number of reverted Certificate] |
| Revocation Date | [Time and date of Certificate revocation] |

| | |
|---|---|
| Reason code | Revocation Reason:<br>unspecified, keyCompromise, cACompromise, affiliate Changed, superseeded, 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<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| This update / Valid from | [Time and date of CRL issuance] |
| Next update | [Time and date of next CRL update] |
| Signature Algorithm | sha256RSA |
| **Extension** | **Value** |
| Authority Key Identifier | 47 ec b0 33 2e 1a 73 b9 f6 42 2e c5 00 09 73 1f c8 b4 76 f4 |
| CRL Number | [Unique Increasing Number per CRL] |
| Approx. Version | Starting from: V2.2 |
| Next CRL Publish | [Time and date of next CRL publish] |
| **Reverted Certificates** | **Value** |
| Certificate Serial Number | [Serial Number of reverted Certificate] |
| Revocation Date | [Time and date of Certificate revocation] |
| Reason code | Revocation Reason:<br>unspecified, keyCompromise, cACompromise, affiliate Changed, superseeded, 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<br>O = Commerzbank AG<br>L = Frankfurt/Main<br>C = DE |
| This update / Valid from | [Time and date of CRL issuance] |
| Next update | [Time and date of next CRL update] |
| Signature Algorithm | sha256RSA |
| **Extension** | **Value** |

| | |
|---|---|
| Authority Key Identifier | af ff f0 ee f9 c7 a6 fe b7 02 ac 80 5e ce fa b6 87 dd 6d 5d |
| CRL Number | [Unique Increasing Number per CRL] |
| Approx. Version | Starting from: V1.1 |
| Next CRL Publish | [Time and date of next CRL publish] |
| **Reverted Certificates** | **Value** |
| Certificate Serial Number | [Serial Number of reverted Certificate] |
| Revocation Date | [Time and date of Certificate revocation] |
| Reason code | Revocation Reason:<br>unspecified, keyCompromise, cACompromise, affiliate Changed, superseeded, cessationOfOperation, certificateHold, removeFromCRL |

#### 7.2.1. Version Number(s)

Commerzbank Root CA issues CRLs based on X.509 version 2.

#### 7.2.2. CRL and CRL Entry Extensions

CRL Extensions can be found in the CRL profile currently valid for Commerzbank Root CA 2. See also 7.2. CRL profiles.

### 7.3. OCSP Profile

not applicable. OCSP is not supported by Commerzbank Persons PKI.

#### 7.3.1. Version Number(s)

not applicable.

#### 7.3.2. OCSP Extensions

not applicable.

# 8. Auditing and verification of compliance

Within the framework of Commerzbank Persons PKI, internal audits are carried out in order to identify deviations from the regular operations of Commerzbank PKI from the statements in the Commerzbank Certificate Policy or Certification Practice Statement (CP/CPS), and to take necessary corrective measures in the event of any deviations from the conformity detected.

## 8.1. Frequency and circumstance of the check

In principle, internal audits and reviews are planned at regular intervals. Frequency and circumstances that may lead to a check are determined by Commerzbank Revision.

## 8.2. The identity and qualification of the auditor

It is planned that only internal Commerzbank AG employees carry out the conformity check. The audit staff should have knowledge from auditing in the security environment, in particular the necessary knowledge from the area of public key infrastructure (PKI) and from the area of data center operation (ITIL certification) is required.

## 8.3. The ratio of the reviewer to the entity being reviewed

The assigned auditor for checking compliance is organizationally independent of the audited entity, namely Commerzbank AG Persons PKI (technology and processes).

## 8.4. Areas covered by the review

The areas affected by a review are determined by Commerzbank Audit. Certain areas can be defined from the outset for circumstances that make it absolutely necessary to carry out a review.

These include:

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

## 8.5. Measures in the event of non-compliance or deviate from compliance

If deviations from the conformity are found, they must be corrected promptly. To this end, an action plan is being developed which describes the necessary measures to carry out the necessary corrections.

Once the action plan has been implemented, it must be checked whether the measures implemented have led to a correction of the deficiencies. Commerzbank IT Management and Commerzbank Audit are informed of the results achieved.

## 8.6. Communication of test results

The results of the audit are considered confidential and are not intended for the public.

# 9. Other legal and business regulations

This section refers to the business, legal and data protection aspects of Commerzbank Personal PKI.

## 9.1. Fees

The fees for services provided by the certification authorities operated by Commerzbank AG can be found in the internal billing table. This can be obtained from the contact person specified in section 1.5.2.

### 9.1.1. Fees for issuing and renewing certificates

Detailed information can be found in the Commerzbank internal billing table for the Persons PKI service.

### 9.1.2. Fees for accessing certificates

Detailed information can be found in the Commerzbank internal billing table for the Persons PKI service.

### 9.1.3. Fees for accessing revocation lists or status informations

Detailed information can be found in the Commerzbank internal billing table for the Persons PKI service.

### 9.1.4. Fees for additional services

Detailed information can be found in the Commerzbank internal billing table for the Persons PKI service.

### 9.1.5. Policy for reimbursement of fees

Detailed information can be found in the Commerzbank internal billing table for the Persons PKI service.

## 9.2. Financial responsibility

### 9.2.1. Insurance coverage

Insurance coverage is not provided.

### 9.2.2. Assets

Assets are not covered.

### 9.2.3. Insurance cover or warranty for certificate holders

There is no insurance cover for certificate holders.

## 9.3. Business Information Confidentiality

### 9.3.1. Sensitive information

Any information about participants and applicants not covered by 9.3.2 is classified as confidential information. This information includes, but is not limited to Business plans, sales information, business partner information, and any information that was known during the registration process.

#### 9.3.2. Confidential informations are not considered

Any information contained or derived from the certificates and revocation lists issued explicitly (e.g. e-mail address) or implicitly (e.g. data on certification) is classified as non-confidential.

#### 9.3.3. Responsibility to protect confidential information

Each CA operating within Commerzbank Persons PKI is responsible for measures to protect confidential information.

### 9.4. Data protection (personal)

#### 9.4.1. Privacy Policy/plan

The storage and processing of personal data depends on the legal data protection regulations.

#### 9.4.2. Confidential Information

All information about the certificate holder and the applicant must be kept confidential.

#### 9.4.3. Non-confidential information

Information contained in the public certificates, such as the Commerzbank certificate or the certification authority certificate, is not confidential. It also applies to information contained in the public certificate revocation lists (CRLs).

#### 9.4.4. Responsibility for the protection of personal information

Commerzbank PKI operations are responsible for protecting confidential information. Disclosure of confidential information can only be made in consultation with the responsible authorities. More information can be obtained from the Crypto Services cell.

#### 9.4.5. Notification of use of personal information

The certificate holder agrees to the use of personal data by a certification authority, as far as this is necessary for the provision of services. In addition, any information that is treated as non-confidential may be published.

#### 9.4.6. Disclosure in the event of a court order or judicial evidence

Commerzbank AG complies with the statutory data protection regulations when storing and processing personal data. Disclosure will only be made to state authorities if appropriate orders have been issued.

#### 9.4.7. Other circumstances of a publication

None.

### 9.5. Copyright

Commerzbank AG owns the copyrights for issued documentation within the framework of the Persons PKI.

## 9.6. Commitments

### 9.6.1. Obligations of the certification authorities

Commerzbank AG certification authorities undertake to comply with the established provisions of the CP or CPS documentation.

### 9.6.2. Registration Authority Obligation

Commerzbank AG registration authorities undertake to comply with the established provisions of the CP or CPS documentation.

### 9.6.3. Obligation of the certificate holder

The use of the certificates by the certificate holder must follow the "Commerzbank guidelines for the use of certificates". In Chapter 1.4. The scope of application of certificates is defined for the permissible and illegal applications of the keys or certificates. In addition, when using the private keys, the certificate holder must fulfill his obligations as defined in the certificate policy.

### 9.6.4. Obligation of the trusting party

The use of the certificates by trusting parties must comply with the assigned certificate policies of his organization. The permissible and illegal applications of the keys or certificates are defined there.

### 9.6.5. Commitment of other participants

Not applicable as no other participants are provided.

## 9.7. Warranty

In principle, no warranty is assumed. Commerzbank AG provides the necessary IT resources for the operation of the PKI, but without guaranteed availability.

## 9.8. Limitation of Liability

Commerzbank AG assumes no liability for property damage and financial losses. In particular, any liability toward third parties shall be lost in the event of improper or grossly negligent use of Commerzbank Persons PKI.

## 9.9. Indemnification

Commerzbank AG is not liable for incorrect use of the certificate and the underlying private key or use of the key material based on incorrect or incorrect information when applying for it.

## 9.10. Entry into force and repeal

### 9.10.1. Entry into force

This will take effect once the current Commerzbank CP/CPS documentation has been published. The publication takes place at the URL specified in the certificate:

http://ca.commerzbank.com/cpcps.en.html

### 9.10.2. Cancellation

This document is valid until

- It is replaced by a new version or
- The operation of Commerzbank AG certification authorities is discontinued.

#### 9.10.3. Consequences of suspension

None.

## 9.11. Individual notification and communication with participants

The individual notification of Commerzbank Persons PKI Participants is made by the distribution and approval of the "Commerzbank Guidelines for the Use of Certificates".

## 9.12. Amendments to the Directive

The addition and modification of the CP or CPS documentation is in the responsibility of the Crypto Services cell. See Section 1.5 for contact details.

#### 9.12.1. Process for completing the policy

Not applicable.

#### 9.12.2. Notification method and time period

Not applicable.

#### 9.12.3. Conditions for changing an OID

Not applicable.

## 9.13. Arbitration

Not applicable.

## 9.14. Jurisdiction

The operation of Commerzbank Persons PKI is subject to the laws of the Federal Republic of Germany. The place of jurisdiction is Frankfurt/Main, Federal Republic of Germany. This place of jurisdiction also applies to parties whose domicile or the usual place of residence is transferred abroad or is unknown.

## 9.15. Compliance with applicable law

Certificates issued by Commerzbank Persons PKI are not compliant with qualified certificates. The specifications and guidelines set out in the signature set [SigG] are therefore not binding for the operation of Commerzbank Persons PKI.

## 9.16. Other regulations

#### 9.16.1. Completeness

All regulations described in the CP & CPS for the Persons PKI apply between the certification authorities operated by Commerzbank AG and their certificate holders. The output of a new version replaces all previous versions. Verbal agreements or ancillary agreements are not permitted.

### 9.16.2. Transfer of rights

No transfer of rights is foreseen.

### 9.16.3. Severability

Should individual provisions of this CP & CPS rulebook be invalid or contain gaps in this rulebook, the validity of the remaining provisions is not affected.

In place of the invalid provisions, the effective provision shall be deemed to have been agreed, which corresponds to the meaning and purpose of the invalid provision. In the case of gaps, the agreement which would have been reasonably agreed upon in the sense and purpose of this contract would have been considered from the outset.

It is expressly agreed that all provisions of these CP & CPS, which provide for limitation of liability, exclusion or limitation of warranties or other obligations or exclusion of damages, shall exist and be enforced as independent regulations and independent of other provisions.

### 9.16.4. Enforcement clause

Legal disputes arising from the operation of a certification authority operated by Commerzbank AG are governed by the laws of the Federal Republic of Germany.

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

### 9.16.5. Force Majeure

Commerzbank AG assumes no liability for the breach of a duty or for delay or non-performance within the framework of this CPS, provided that this results from events outside its control, such as force majeure, acts of war, epidemics, grid failures, fires, earthquakes and other disasters.

## 9.17. Other regulation

None