COMMERZBANK - X.509 PKI

COMMERZBANK PERSONEN PKI

Zertifikatsrichtlinie
Certificate Policy (CP)
&
Erklärung zum Zertifizierungsbetrieb
Certification Practice Statement (CPS)

Version 1.0

Dokumentenkontrolle:

Titel:	Commerzbank Personen PKI – Personen PKI Certificate Policy (CP) & Certification Practice Statement (CPS)
Beschreibung:	Darstellung der Prozesse und Prozeduren der Commerzbank Personen PKI
RFC Schema:	RFC 3647 (Certificate Policy and Certification Practices Framework)
Autoren:	Ralf Baumgart, Commerzbank AG, GS-ITR 4.3.5 Jung-Uh Yang, Consultant

Versionskontrolle:

Version	Datum	Kommentar
1.0	20.01.2011	Freigabe Version 1.0

Inhalt

1. Einleitung

Der Begriff „Certificate Policy (CP)“, definiert im X.509 Standard, steht für die Gesamtheit der Regeln und Vorgaben, welche die Anwendbarkeit eines Zertifikatstyps festlegen. Die Zielsetzung einer Certificate Policy wird im RFC 3647 („Certificate Policy and Certification Practices Framework“) ausführlich diskutiert. Die CP ist eine Entscheidungshilfe für den Zertifikatsnutzer ob einem bestimmten Zertifikat und Anwendung vertraut werden kann.

Insbesondere sollte eine CP darlegen:

- welche technischen und organisatorischen Anforderungen die bei der Ausstellung der Zertifikate eingesetzten Systeme und Prozesse erfüllen,
- welche Vorgaben für die Anwendung der Zertifikate sowie im Umgang mit den zugehörigen Schlüsseln und Signaturerstellungseinheiten (z.B. Chipkarten) gelten,
- welche Bedeutung den Zertifikaten und zugehörigen Anwendungen zukommt, d.h. welche Sicherheit, Beweiskraft, oder rechtliche Relevanz die mit ihnen erzeugten Ciphertext bzw. Signaturen besitzen.

Das Konzept einer “Certification Practice Statement (CPS)” wurde von der American Bar Association (ABA) entwickelt und ist in deren Digital Signature Guidelines (ABA Guidelines) aufgeführt. Die CPS ist eine detaillierte Beschreibung des Zertifizierungsbertriebes der Organisation. Aus diesem Grund stellen Organisationen, die eine oder mehrere Zertifizierungsstellen betreiben, in der Regel auch eine CPS zur Verfügung. In Rahmen einer unternehmensweiten PKI ist die CPS für Organisationen ein adäquates Mittel um sich selbst zu schützen, sowie Geschäftsvorfälle zu Zertifikatsnehmern und vertrauenden Parteien darzustellen.

Ein zentraler Aspekt der Commerzbank CP/CPS der Commerzbank Personen PKI ist die Bestimmung der Vertrauenswürdigkeit auszugebender Zertifikate und des Zertifizierungsdienstes betrieben durch das Rechenzentrum des Commerzbank. Mit Teilnahme an den Commerzbank Zertifizierungsdiensten akzeptieren die Commerzbank Mitarbeiter und vertrauende Parteien die Bedingungen und Regularien aufgeführt im CP/CPS.

Die Dokumentenstruktur orientiert sich an dem im RFC 3647 angegebenen Empfehlungen. Entsprechend den Vorgaben des RFC 3647 legt die Commerzbank CP/CPS der Commerzbank Personen PKI die Vorgehensweise dar, die der Zertifizierungsdienst bei der Beantragung, Generierung, Auslieferung und Verwaltung der Zertifikate anwendet.

Aufgrund der Anforderung einer vereinfachten Dokumentenverwaltung wurden die CP (Certficate Policies) und CPS (Certification Practice Statement) in einem zentralen Dokument zusammenzufassen. Dieses Dokument beschreibt die Zertifikatsrichtlinie und die Erklärung zum Zertifizierungsbetrieb der PKI der Commerzbank AG. Die Verteilung dieses Dokuments ist kostenfrei und öffentlich zugänglich.

1.1. Überblick

Ein zentraler Aspekt der Commerzbank CP/CPS der Commerzbank Personen PKI ist die Bestimmung der Vertrauenswürdigkeit auszugebender Zertifikate und des Zertifizierungsdienstes betrieben durch das Rechenzentrum des Commerzbank. Mit Teilnahme an den Commerzbank Zertifizierungsdiensten akzeptieren die Commerzbank Mitarbeiter und vertrauende Parteien die Bedingungen und Regularien aufgeführt im CP/CPS.

Die Dokumentenstruktur orientiert sich an dem im RFC 3647 angegebenen Empfehlungen. Entsprechend den Vorgaben des RFC 3647 legt die Commerzbank CP/CPS der Commerzbank Personen PKI die Vorgehensweise dar, die der Zertifizierungsdienst bei der Beantragung, Generierung, Auslieferung und Verwaltung der Zertifikate anwendet.

Aufgrund der Anforderung einer vereinfachten Dokumentenverwaltung wurden die CP (Certficate Policies) und CPS (Certification Practice Statement) in einem zentralen Dokument zusammenzufassen. Dieses Dokument beschreibt die Zertifikatsrichtlinie und den Zertifizierungsbetrieb der Commerzbank AG X.509 – Personen PKI Lösung. Die Verteilung dieses Dokuments ist kostenfrei und öffentlich zugänglich für Commerzbank Mitarbeiter.

1.1.1. Commerzbank Personen PKI Architektur

Die Commerzbank AG betreibt Zertifizierungsdienste für die Erzeugung, Ausgabe und Verwaltung von Zertifikaten. Die Commerzbank PKI erlaubt die kontrollierte Ausgabe von Zertifikaten bzw. Smart Cards.

Commerzbank Benutzer erhalten Zertifikate und Smart Cards kontrolliert und verwaltet durch ein Zertifikats- und Smart Card Managementsystem. Commerzbank Smart Card Zertifikate und Zertifikate für Gruppenpostfächer/Ressourcen Postfächer werden in Namen der Commerzbank Antragsteller durch die Personen PKI beantragt.

Darüber hinaus werden CA Zertifikate ausgestellt zur Zertifizierung der Wurzel-Zertifizierungsstelle **Commerzbank AG Inhouse Root CA** selbst und der untergeordneten **Commerzbank AG Inhouse Sub CA 03**.

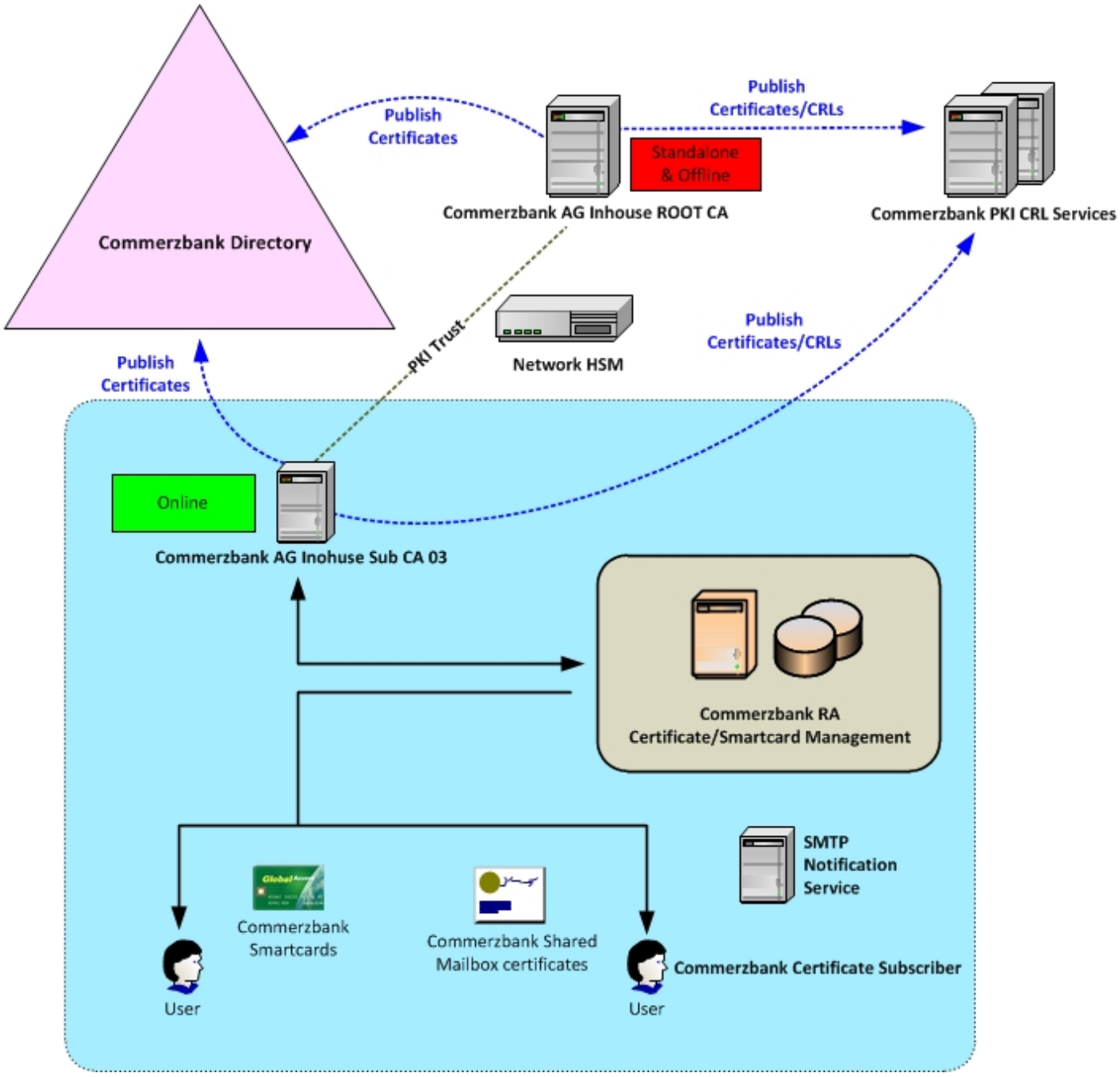
Ein Netzwerk Hardware Security Modul, kurz HSM, übernimmt die Schlüsselgenerierung und -verwaltung für die Commerzbank Zertifizierungsstellen und für das Zertifikatsmanagement.

Die Commerzbank Zertifizierungsinfrastruktur ist hierarchisch aufgebaut und terminiert an der **Commerzbank AG Inhouse Root CA**. Weitergehende Informationen zur Personen PKI Architektur können auf Wunsch angefordert werden. Die Kontaktinformationen sind aus Kapitel 1.5.2. Kontaktpersonen zu entnehmen.

Anmerkung: Es existiert eine weitere CP/CPS Dokumentation zur Commerzbank Inhouse Gateway CA. Da sowohl die Commerzbank Personen PKI, als auch die Commerzbank Gateway PKI an derselben Commerzbank AG Inhouse Root CA terminieren, ist diese Wurzelzertifizierungsinstanz auch in beiden Commerzbank CP/CPS Dokumentation erwähnt.

Es sind weitere Zertifizierungsstellen in der Commerzbank PKI Umgebung etabliert, die aber keine Außenwirkung haben. Daher wurden diese CA Komponenten in den aktuellen CP/CPS Beschreibungen für die Commerzbank Gateway PKI als auch für die Commerzbank Personen PKI nicht aufgeführt.

Commerzbank Personen PKI



1.2. Dokumententitel und Identifikation

Dies ist die Commerzbank AG *"Certification Practice Statement and Certificate Policy"* für die Commerzbank Personen PKI. Ein eindeutiger ASN.1 Object Identifier (OID) ist diesem Dokument zugewiesen.

Die Commerzbank OID ist bei der IANA.ORG registriert, siehe auch:

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

Commerzbank Enterprise OID: 1.3.6.1.4.1.14978

OID Beschreibung: Commerzbank SMI Network Management Private Enterprise Code

Commerzbank PKI OID: 1.3.6.1.4.1.14978.5

OID Beschreibung: Namensraum der X.509 PKI Dienste der Commerzbank AG

Der CP/CPS Titel lautet:

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

Commerzbank CP/CPS OID: 1.3.6.1.4.1.14978.5.1

OID Beschreibung: OID für die Commerzbank AG Certificate Policy & Certification Practice Statement Dokumentation

Commerzbank CP/CPS OID: 1.3.6.1.4.1.14978.5.1.3

OID Beschreibung: OID für die Commerzbank Personen PKI – Certificate Policy & Certification Practice Statement

Die Lokation der Commerzbank AG CP/CPS Dokumentationen für Commerzbank Zertifikatsnehmer und vertrauende Parteien lautet: http://ca.commerzbank.com/cps/cps.htm

Die Commerzbank betreibt die Zertifizierungsstellen in einer 2-stufigen (2-tier) Architektur. Die Eindeutigkeit der Zertifizierungsstellen wird durch den „Distinguished Name“ der Zertifizierungsstellen gewährleistet.

Der vollständige DN der Commerzbank Inhouse Root CA lautet:

- **Commerzbank AG Inhouse Root CA**

  CN=Commerzbank AG Inhouse Root CA,

  O=Commerzbank AG,

  L=Frankfurt am Main,

  C=DE

Der vollständige DN der Commerzbank AG Sub CA 03 lautet:

- **Commerzbank AG Inhouse Sub CA 03**

  CN=Commerzbank AG Inhouse Sub CA 03,

  O=Commerzbank AG,

  L=Frankfurt am Main,

  C=DE

1.3. Teilnehmer und Instanzen

Die Teilnehmer der Commerzbank Personen PKI sind grundsätzlich in 4 Teilnehmergruppen klassifiziert. Jeder dieser teilnehmenden Gruppen bietet PKI Dienste und Ressource an oder konsumiert PKI Dienste und Ressourcen.

Zertfizierungsstelle oder Certificate Authority (CA):

- Ausstellen von Zertifikaten;
- Sperren von Zertifikaten;
- Wiederherstellen von Benutzerschlüssel

Registrierungsstelle oder Registration Authority (RA):

- Identifizierung von Benutzer oder Maschinen;
- Registrierung Benutzer oder Maschinen;
- Beantragung einer Zertifikatsanforderung für andere Benutzer
- Beantragung einer Sperranforderung von Zertifikaten

Zertifikatsnehmer:

- Konsumiert Zertifikate und PKI Dienstleistungen

Vertrauende Parteien (z. B. e-Mail Empfänger):

- Konsumiert PKI Dienstleistungen

1.3.1. Zertifizierungsstellen

Das 2-Tier CA Hierarchie-Modell basiert auf:

- ***Offline Commerzbank AG Inhouse Root CA*** mit einem selbst-signierten CA Zertifikat. Die Commerzbank Root CA ist von Produktionsnetz entkoppelt und unterhält eine dedizierte Verbindung zum Network Hardware Security Module (HSM). Alle kryptographischen Operationen der Commerzbank Root CA werden durch das HSM ausgeführt.
  Die Commerzbank Root CA stellt CA Zertifikate und Sperrlisten für subordinierte Zertifizierungsstelleninstanzen (Commerzbank AG Sub CA), wie auch für sich selbst aus.
- ***Online Commerzbank AG Inhouse Sub CA 03*** mit einem von der Commerzbank Root CA ausgestellten Zertifikat. Die Commerzbank AG Inhouse Sub CA 03 ist mit dem Produktionsnetz verbunden und unterhält ebenso, wie die Commerzbank Root CA, eine dedizierte Verbindung zur Network HSM. Alle kryptographischen Operationen der Commerzbank AG Inhouse Sub CA 03 werden durch das HSM ausgeführt. Die Commerzbank Sub CA 03 stellt End-Entitäten Zertifikate (für Commerzbank Smart Cards und Commerzbank Gruppenpostfächer) und Sperrlisten für die Zertifikatsnehmer aus.

Für die Commerzbank AG Zertifizierungsstellen sind folgende Lebensdauern festgelegt:

Commerzbank AG Inhouse Root CA

- Root CA Zertifikat: 30 Jahre
- Root CA CRLs: 4 Monate

Commerzbank AG Inhouse Sub CA 03

- Sub CA 03 Zertifikat: 10 Jahre
- Sub CA 03 CRLs: 14 Tage

1.3.2. Registrierungsstellen

Die Registrierungsstelleninstanzen im Sinne dieser Certificate Policy sind Instanzen, welche die Zertifikatsnehmer und Antragssteller erfassen und identifizieren und auch für Zertifikatsnehmer Zertifikate beantragen. Die Registrierung der Mitarbeiter-Zertifikate geschieht in lokalen Registrierungsstellen (LRA). Diese sind unterstützend für den Zertifizierungsbetrieb der X.509 basierenden PKI verantwortlich. Die zentrale Aufgabenstellung ist die Bereitstellung von externen Teilnehmerzertifikaten für die Kommunikation zu den vertrauenden Parteien.

Die Zertifikatsbeantragung für die Zertifikatsnehmer erfolgt über ein Registrierungswerkzeug, welches eine kontrollierte Ausgabe von Zertifikaten auf Smart Cards ermöglicht. Darüber hinaus wird die gesamte Lebenszyklusverwaltung von Zertifikaten und Smart Cards durch dieses Werkzeug organisiert. Die Erstantragsstellung wird nicht selbst durch den Zertifikatsnehmer ausgeführt.

1.3.3. Zertifikatsnehmer

Sind End-Entitäten denen ein Zertifikat durch die Commerzbank Inhouse Sub CA 03 zugewiesen wird. Schlüsselgenerierung und Zertifikatsausgabe unterstehen nicht der Kontrolle des Zertifikatsnehmers, sondern obliegen der Personen PKI.

End-Entitäten als Zertifikatsnehmer in Rahmen dieser PKI stellen Commerzbank Vollzeit-Mitarbeiter, Teilzeitbeschäftigte, technische Systeme (wie z. B.: Mailbox für eine Web-Anwendung), und im Bedarfsfall auch für Geschäftspartner und auch externe Mitarbeiter dar, denen ein S/MIME Zertifikat durch das Personen PKI zugewiesen wurde.

1.3.4. Vertrauende Parteien

Vertrauende Parteien im Sinne der vorliegenden Certificate Policy sind alle Personen und Systeme, die mit Hilfe eines Zertifikates mit dessen Inhaber sicher kommunizieren wollen. In der Regel stellen die vertrauenden Parteien eMail Empfänger von SMIME geschützten Nachrichten dar. Vertrauende Parteien sind keine Commerzbank Mitarbeiter oder Teilnehmer, die durch die Commerzbank Zertifikate bzw. Smart Cards bezogen haben.

1.3.5. Weitere Teilnehmer

Nicht zutreffend.

1.4. Anwendungsbereich von Zertifikaten

Die Verwendung von Schlüsseln und Zertifikaten obliegt der Verantwortung des Zertifikatsnehmers und der vertrauenden Partei.

1.4.1. Zulässige Anwendung von Zertifikaten

Die im Rahmen dieser CP/CPS ausgestellten Smart Card Zertifikate können durch den Zertifikatsnehmer für die **Authentifikation** (z. B. Windows Anmeldung), als auch zur ***Verschlüsselung und Signatur*** herangezogen werden können.

Bei Gruppenpostfächer dienen die Zertifikate ausschließlich für die **Verschlüsselung** von Emails.

Folgende Tabelle beschreibt den Anwendungsbereich der ausgestellten Zertifikate:

Ausgestellt von der Commerzbank AG Inhouse Root CA:

Zertifikatstyp	**Anwendungsbereich des ausgegebenen Zertifikats**
Certification Authority	ROOT CA Zertifikat für selbst signierte (Wurzel-) Zertifizierungsstellen

Ausgestellt von der Commerzbank AG Inhouse Root CA:

Zertifikatstyp	**Anwendungsbereich des ausgegebenen Zertifikats**
Subordinate Certification Authority	CA Zertifikat für subordinierte Zertifizierungsstellen

Ausgestellt von der Commerzbank Inhouse Sub CA 03:

Zertifikatstyp	Anwendungsbereich des ausgegebenen Zertifikats
Coba SC Authentication	Smart Card Authentifikationszertifikat für die Anmeldung, z. B. Windows Logon
Coba SC Encryption	Smart Card Verschlüsselungszertifikat für die Verschlüsselung, z. B. für Verschlüsselung von eMails
Coba SC Signature	Smart Card Signaturzertifikat für die elektronische Signatur, z. B. für die Signierung von eMails
Commerzbank Soft PSE Encryption	Software Verschlüsselungszertifikat für die Verschlüsslung von eMails für Gruppenpostfächern.
"Zertifikate für das Zertifikatsmanagmentsystem"	Zusätzlich wurde für den Betrieb des Zertifikatsmanagementsystems Softwarezertifikate zur technischen Nutzung innerhalb des Systems erstellt

1.4.2. Unzulässige Anwendung von Zertifikaten

Die Zertifikatsnutzung von Benutzerzertifikaten in Rahmen der Commerzbank Personen PKI ist beschränkt auf:

- Authentifikation
- Verschlüsselung
- Elektronische Signierung

Die Zertifikatsnutzung von CA Zertifikaten in Rahmen der Commerzbank Personen PKI ist beschränkt auf:

- Signierung von CA Zertifikaten für die Commerzbank Inhouse Root CA
- Signierung von End-Entitäten Zertifikaten für die Commerzbank Inhouse Sub CA 03

Eine Anwendung der Zertifikate für den privaten Gebrauch ist ebenso untersagt, wie auch die Nutzung dieser Zertifikate für andere Anwendungszwecke abweichend von 1.4.1 Zulässige Anwendungen von Zertifikaten.

Jegliche weitere Zertifikatnutzung ist untersagt, insbesondere die Zertifizierung weiterer, untergeordneter Zertifizierungsstellen ist ausschließlich der Commerzbank Inhouse Root CA Zertifizierungsstelle vorbehalten, als auch die Nutzung von Commerzbank Zertifikaten für die qualifizierte elektronische Signatur.

Zum Schutz der Commerzbank CP/CPS Konformität ist jegliche Änderung oder Erweiterung der Zertifikatsanwendung unverzüglich der Commerzbank PKI Administration anzuzeigen.

1.5. Verwaltung der Richtlinien

1.5.1. Organisation

Die Commerzbank AG ist die verantwortliche Organisation für die Richtlinien Verwaltung.

Commerzbank AG,
60261 Frankfurt am Main,
Deutschland

1.5.2. Kontaktpersonen

Folgende Personen sind Ansprechpartner für die Commerzbank Personen PKI:

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

1.5.3. Verantwortliche Personen für das CPS

Die Commerzbank AG, GS-ITR 4.3, ist verantwortlich für die Einhaltung des Zertifizierungsbetriebes und -richtlinien gemäß der CP/CPS und begleitender Dokumentation. Ansprechpartner zur Einhaltung der CP/CPS sind im Abschnitt 1.5.2. Kontaktpersonen aufgeführt.

1.5.4. CPS Genehmigungsverfahren

Die Commerzbank AG, GS-ITR 4.3, ist verantwortlich für die Freigabe dieser CP/CPS. Die CP/CPS Dokumentation wird fortwährend auf Konformität hin untersucht.

1.6. Definitionen und Abkürzungen

ABA (American Bar Association) – Verband der amerikanischen Revisoren

ASN.1 (Abstract Syntax Notation) – Abstrakte Syntaxnotation Nummer 1, Datenbeschreibungssprache

C (Country) – Landesobjekt (Teil des X.500 Distinguished Name), für Deutschland C=DE

CA (Certification Authority) – Zertifizierungsstelle

CN (Common Name) – Namensobjekt (Teil des X.500 Distinguished Name)

CP (Certificate Policy) – Zertifikatsrichtlinie

CPS (Certification Practice Statement) – Zertifizierungsbetrieb

CRL (Certificate Revocation List) – Liste, in der eine Zertifizierungsstelle die von ihr ausgestellten Zertifikate, die gesperrt aber noch nicht abgelaufenen sind, veröffentlicht

CSR (Certificate Signing Request) – Signierte Zertifikatsanforderung

DN (Distinguished name) – Eindeutiger Name basiert auf der X.500 Namensbildung

DNS (Domain Name System) – Standard für Internet Namen

FIPS (Federal Information Processing Standard) – Kryptographiestandard der US Behörden

HSM (Hardware Security Module) – Hardwarekomponente, das sicherheitsrelevante Informationen wie Daten und kryptographische Schlüssel sicher speichert und verarbeitet

IETF (Internet Engineering Task Force) – Projektgruppe für die technische Weiterentwicklung des Internets. Spezifiziert quasi Standards in Form von RFCs

IP (Internet Protocol) – Internetprotokoll

ISO (International Organization for Standardization) – Internationale Normungsstelle

ITU (International Telecommunications Union) – Standardisierungsgremium, hat auch X.509 spezifiziert

LDAP (Lightweight Directory Access Protocol) – Zugriffsprotokoll für Verzeichnisdienste

NIST (National Institute of Standards and Technology) – Normungsstelle der Vereinigten Staaten

O (Organization) – Objekt für die Organisation (Teil des X.500 Distinguished Name)

OID (Object Identifier) – Object Identifikator, eindeutige Refrenz zu Objekten im OID Namensraum

OU (Organizational Unit) – Objekt für die Organisationseinheit (Teil des X.500 Distinguished Name)

PIN (Personal Identification Number) – Geheimzahl zur Authentisierung eines Individuums z.B. gegenüber einer Chipkarte

PKCS (Public key Cryptographic Standard) – Serie von Quasi-Standards für kryptographische Operationen spezifiziert durch RSA

PKI (Public Key Infrastructure) – Beschreibung von Technologie, Prozesse und Teilnehmer in Rahmen der asymetrischen Kryptographie

PKIX (Public Key Infrastructure eXchange) – eine Serie von Spezifikationen der IETF im Umfeld von digitalen Zertifikaten nach X.509 Spezifikation

RA (Registration Authority) – Registrierungsstelle

RFC (Request For Comment) – Quasi Internet-Standard ausgegeben durch die IETF

URL (Uniform Resource Locator) – Ressourcen Lokation im Internet

X.500 – Protokolle und Dienste für ISO konforme Verzeichnisse

X.509 – Authentifikationsmethode für X.500 Verzeichnisse

X.509v3 – Aktuell gültiger PKI Zertifikatsstandard

2. Publikationen und Informationsdienste

2.1. Verzeichnis- und Informationsdienste

Die Commerzbank Personen PKI nutzt seinen internen Verzeichnisdienst für die sichere Email Kommunikation. Die hierzu notwendigen Empfängerzertifikate werden durch die Personen PKI verwaltet.

Öffentliche Informationen wie Commerzbank CA Zertifikate, CRLs und CP/CPS Dokumentation wird ein webbasierter Dienst als Informationsdienst genutzt. Ebenso werden CA Informationen mit Ausnahme der CP/CPS Dokumentation im Commerzbank Verzeichnisdienst veröffentlicht.

2.2. Publikation von Zertifizierungsinformationen

Die Publikation der Verschlüsselungs-Zertifikate (eMail Empfängerzertifikate) erfolgt automatisiert durch die Personen PKI in den lokalen Verzeichnisdienst. Hierzu ist keine Benutzerintervention ist notwendig. Externe Empfängerzertifikate für die sichere E-Mail Kommunikation werden durch einen vorgelagerten Austausch von Empfängerzertifikaten gewährleistet.

Die fortwährende Publikation der CRLs auf den Commerzbank PKI CRL Web Servern wird durch die Commerzbank AG Inhouse Sub CA 03 automatisiert durchgeführt; die Publikation der Commerzbank AG Inhouse Root CA wird im Gegensatz manuell durch Mitarbeiter von GS-ITR 4.3 auf den Web Servern ausgeführt, da eine netztechnische Trennung bzw. ein offline Betrieb adressiert wird. Commerzbank CA Zertifikate und die CP/CPS Dokumentation wird durch die GS-ITR 4.3 freigegeben und auf den entsprechenden Web Lokation eingestellt.

Folgende Veröffentlichungsorte sind vorgesehen:

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

2.3. Veröffentlichungsintervall

Die Veröffentlichung der Commerzbank Certificate Policies und des Certification Practice Statements erfolgt jeweils nach ihrer Erstellung bzw. Aktualisierung.

Die Veröffentlichung der Commerzbank CA Zertifikate erfolgt einmalig nach der Installation der Commerzbank Zertifizierungsstellen. Eine erneute Publikation erfolgt nur bei Ablauf bzw. Erneuerung der CA Zertifikats.

CRL oder Sperrlisten werden nach vorgeschriebenem Publikationsintervall erzeugt und sofort auf den PKI CRL Web Diensten publiziert.

CRLs durch die Root CA ausgestellt:	3 Monate mit einer Überlappung von 1 Monat
CRLs durch die Sub CA 03 ausgestellt:	wöchentlich mit einer Überlappung von 7 Tagen

Das Veröffentlichungsintervall der externen Empfängerzertifikate durch den Commerzbank Registration Authority Officer ist nach einem definierten Prozess festgelegt. Entsprechende Prozessinformationen zum Personen PKI können bei Bedarf von der GS-ITR 4.3 erfragt werden.

2.4. Zugang zu den Informationsdiensten

Der Zugriff auf die Commerzbank CA Zertifikate, CRLs und der CP/CPS Dokumentation ist nicht eingeschränkt und daher öffentlich. Siehe auch Veröffentlichungsorte in Abschnitt 2.2. Publikation von Zertifizierungsinformationen.

3. Identifikation and Authentifikation

3.1. Namen

3.1.1. Namensform

Der X.500 Distinguished Name in den CA-Zertifikaten für Commerzbank Zertifikatsnehmer ist wie in den folgende Tabellen dargestellt, spezifiziert. Der Einsatz von DNs für die Benennung im Subject Name Field erlaubt die Eineindeutigkeit der Namensvergabe von Zertifizierungsstellen innerhalb der Commerzbank AG.

Das Schema für die Namensform ist bei allen ausgestellten Zertifikaten der Commerzbank AG Inhouse Root CA identisch und folgt untenstehendem Regelwerk:

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

In der tatsächlichen Umsetzung der Zertifizierungsstelleninfrastruktur werden nicht alle (Namens-) Attribute festgelegt, da die Aussagekraft und Eindeutigkeit der Namen für die Zertfizierungsstellen mit den dafür notwendigen Attributen als ausreichend erachtet wird.

3.1.1.1. Commerzbank AG Inhouse Root CA DN

Der X.500 Distinguished Name der selbst-signierten Commerzbank AG Inhouse Root CA lautet:

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

3.1.1.2. Commerzbank AG Inhouse Sub CA 03 DN

Der X.500 Distinguished Name im Zertifikat der Commerzbank AG Inhouse Sub CA 03, welches durch die Commerzbank Inhouse Root CA ausgestellt wird, lautet:

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

Das Schema für die Namensform ist bei allen ausgestellten Zertifikaten der Commerzbank AG Inhouse Sub CA 03 identisch und folgt untenstehendem Regelwerk:

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

3.1.1.3. Commerzbank AG Smart Card Zertifikate DN

Der X.500 Distinguished Name im Zertifikat für die End-Entitäten **Coba SC Authentication**, welches durch die Commerzbank Inhouse Sub CA 03 ausgestellt wird, lautet:

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

State or Province	***
Country	DE

Das Commerzbank Smart Card Zertifikat für die Authentifikation wird nur in der Commerzbank Infrastruktur verwendet und nicht nach außen publiziert.

Der X.500 Distinguished Name im Zertifikat für die End-Entitäten **Coba SC Encryption**, welches durch die Commerzbank Inhouse Sub CA 03 ausgestellt wird, lautet:

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

Der X.500 Distinguished Name im Zertifikat für die End-Entitäten **Coba SC Signature**, welches durch die Commerzbank Inhouse Sub CA 03 ausgestellt wird, lautet:

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

3.1.1.4. Commerzbank AG Zertifikate für Gruppenpostfächer DN

Der X.500 Distinguished Name im Zertifikat für die End-Entitäten
Commerzbank Soft PSE Encryption, welches durch die Commerzbank Inhouse Sub CA 03 ausgestellt wird, lautet:

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

3.1.2. Anforderung an die Bedeutung von Namen

Der Distinguished Name muss den Zertifikatnehmer eindeutig identifizieren. Ist der DN nicht ausreichend, kann zur Einhaltung der Eindeutigkeit eines Namens auch der Subject Alternative Name herangezogen werden. Bei der Namensvergabe sind folgenden Regelungen wirksam:

- Zertifikate dürfen nur auf einen zulässigen Namen des Zertifikatnehmers ausgestellt werden.
    - Bei Authentifikationszertifikaten für Benutzer ist es der Common Name des Benutzers und der UPN (User Principle Name) im Subject Alternative Name Feld des Zertifikatsnehmers.
    - Bei den Verschlüsselungs- und Signaturzertifikaten für Benutzer ist es der Nachname, Vorname im Common Name und die eMail-Adresse im Subject Alternative Name Feld des Zertifikatsnehmers.
    - Bei Verschlüsselungszertifikaten für die Gruppenpostfächern ist es der Gruppenpostfachname im Common Name und die Gruppenpostfach eMail-Adresse im Subject Alternative Name Feld.
- Der DN der Commerzbank Zertifizierungsstellen wird durch die Namens-Objekte Common Name, Organization, Locality und Country gebildet. Eine Eindeutigkeit des DNs ist mit diesem zur Verfügung stehenden Namensobjekten zu gewährleisten.
- Der DN der Authentifikationszertifikate wird durch die Namens-Objekte Common Name, Organization, Locality und Country gebildet. Eine Eindeutigkeit des DNs ist mit diesem zur Verfügung stehenden Namensobjekten zu gewährleisten.

- Der DN der Verschlüsselungs- und Signaturzertifikaten wird durch die Namens-Objekte Common Name, Organization, Locality, Country und der e-mail Adresse des Commerzbank Benutzers gebildet. Eine Eindeutigkeit des DNs ist mit diesem zur Verfügung stehenden Namensobjekten zu gewährleisten.
- Der DN der Verschlüsselungszertifikate für Gruppenpostfächer wird durch die Namens-Objekte Common Name, Organization Unit, Organization, Locality, Country und der e-mail Adresse des Gruppenpostfachs gebildet. Eine Eindeutigkeit des DNs ist mit diesem zur Verfügung stehenden Namensobjekten zu gewährleisten.
- Der alternative Name in den Verschlüsselungs- und Signaturzertifikaten enthält die E-Mail Adresse des Inhabers in der Form Vorname.Nachname@commerzbank.com.
- Jedem Zertifikat wird eine eindeutige Seriennummer zugeordnet, welche eine eindeutige und unveränderliche Zuordnung zum Zertifikatnehmer ermöglicht.

3.1.3. Anonymität und Pseudonymität von Zertifikatsnehmern

Abgesehen von technischen Konten (Service Zertifikate für das Managementsystem) oder Gruppen-Mailboxen sind natürliche Zertifikatsnehmer (Personen) nicht anonym noch werden zur Kennung von Zertifikatsnehmern Pseudonyme verwendet. Jedem Zertifikatsnehmer (Personen) können daher die Zertifikate eindeutig zugeordnet werden.

3.1.4. Regeln zur Interpretation verschiedener Namensformen

Die ausgewiesenen Distinguished Names im Zertifikatsprofil folgen dem X.500 Standard.
Die Commerzbank e-Mail Adressen und UPN Einträge im Zertifikatsprofil folgen dem RFC 822 Regelwerk. UPN Namensinformationen müssen UTF-8 encodiert vorliegen.

3.1.5. Eindeutigkeit von Namen

Der komplette Distinguished Name in den von der Commerzbank ausgestellten Zertifikaten erlaubt die Eindeutigkeit von Namen, sowohl der Commerzbank Zertifizierungsstellen als auch der Namen für die Commerzbank Zertifikatsnehmer.

Eine zusätzliche Kennung im alternativen Namensfeld, nämlich die eindeutige Commerzbank e-mail Adresse, Benutzer UPN Informationen und eine eindeutige Seriennummer in den Zertifikaten, berücksichtigt diesen Aspekt.

3.1.6. Erkennung, Authentifikation und Rolle von Warenzeichen

In der Regel beschränkt sich der DN auf natürliche Personen und hat somit keine Relevanz in der Anerkennung von Warenzeichen. Grundsätzlich sind der Zertifikatsnehmer und auch der Zertifizierungsstellenbetreiber verpflichtet, aufgrund der automatisierten Ausstellung von End-Entitäten Zertifikaten, dass der Schutz Warenzeichen gewährleistet wird.

3.2. Identitätsprüfung bei Neuantrag

3.2.1. Verfahren zur Überprüfung des Besitzes von privaten Schlüsseln

Die Schlüsselpaare der Commerzbank Zertifikatsnehmer werden auf der beantragenden Maschine im Falle von Zertifikaten für Gruppenpostfächer bzw. auf Smart Cards für Benutzerzertifikate generiert. Der Besitznachweis für die privaten Schlüssel erfolgt durch die Signierung (mit dem privaten Schlüssel) des PKCS#10-Zertifikatsrequests. Der Certificate Signing Request oder CSR ist die Basis der Überprüfung von privaten Schlüsseln.

Die Schlüsselpaare der Commerzbank Zertifizierungsstellen werden durch das Hardware Security Modul generiert. Der Besitznachweis für die privaten Schlüssel zu den CA Zertifikaten erfolgt durch die Signierung (mit dem privaten Schlüssel) des PKCS#10-Zertifikatsrequests. Der Certificate Signing Request oder CSR ist die Basis der Überprüfung von privaten Schlüsseln.

3.2.2. Authentifikation der Organisation

Nicht zutreffend. Es werden nur individuelle Zertifikate für Commerzbank Beschäftigte oder Zertifikate für Commerzbank Gruppenpostfächer ausgegeben. Eine Zertifizierung von Mitarbeiter aus anderen Organisationen findet nicht statt. Längerfristig bei der Commerzbank tätige externe Mitarbeiter können temporär Smart Cards beantragen.

3.2.3. Authentifikation von Personen

Für die Erstausstattung von Zertifikaten für Benutzer und Gruppenpostfächern findet eine Identitätsprüfung durch die Registrierungsstelle statt. Hierbei werden die notwendigen Maßnahmen ergriffen um die Identität eines Antragsstellers eindeutig festzustellen. Die Detailverfahren zur Identitätsprüfung können aus den Prozessabläufen für die Ausgabe von Smart Cards entnommen werden.

3.2.4. Nicht überprüfte Zertifikatsnehmer Information

Es werden nur die Informationen des Zertifikatsnehmers überprüft, welche notwendig sind in Rahmen der Authentifikation und Identifikation des Zertifikatsnehmers. Andere Informationen des Zertifikatsnehmers werden nicht berücksichtigt.

3.2.5. Prüfung der Berechtigung zur Antragstellung

Für die Ausgabe von Benutzerzertifikaten und Zertifikate von Gruppenpostfächern findet eine Überprüfung der Berechtigung zur Antragsstellung statt. Die Detailverfahren zur Prüfung der Berechtigung können aus den Prozessabläufen für die Ausgabe von Smart Cards entnommen werden.

3.2.6. Kriterien für Cross-Zertifizierung und Interoperation

Nicht zutreffend. Zurzeit ist keine Cross-Zertifizierung mit anderen Organisationen geplant.

3.3. Identifikation and Authentifikation bei Zertifikatserneuerung

Die Identifizierung und Authentifizierung bei einer routinemäßigen Zertifikatserneuerung mit Schlüsselwechsel (d.h. bei der Ausstellung eines neuen Zertifikates zu einem neuen Schlüssel kurz vor dem regulären Ablauf des alten Zertifikates) ist eine erfolgreiche Anmeldung mit der persönlichen Windows Kennung und einem „Einmal“ Kennwort für Commerzbank Benutzer und Gruppenpostfächern ausreichend.

3.3.1. Identifikation und Authentifikation bei routinemäßiger Zertifikatserneuerung

Die Erneuerung von Smart Card bzw. Gruppenpostfach Zertifikaten erfolgt automatisiert durch die Personen PKI und zugehörigen Managementsystems. Betroffene Zertifikatsnehmer werden über die anstehende Erneuerung informiert. Zur Erneuerung wird eine Authentifikation am Zertifikatsmanagementsystems mittels Windows Benutzerkennung und einem „Einmal“ Kennwort erzwungen.

3.3.2. Identifikation und Authentifikation bei Zertifikatserneuerung nach erfolgtem Zertifikatsrückruf

Die Identifizierung und Authentifizierung bei einer Zertifikatserneuerung nach einer Sperrung entspricht der Identifizierung und Authentifizierung bei der initialen Registrierung.

3.4. Identifikation and Authentifikation bei Zertifikatsrückruf

Ein Antragswesen existiert hierzu. Die entsprechend Prozesse für die Identifikation und Authentifikation beim Zertifikatsrückruf sind im Antragswesen beschrieben und niedergelegt. Grundsätzlich können Zertifikatsinhaber/Zertifikatsnehmer die eigenen Zertifikate oder Vorgesetzte Zertifikate zurückziehen. Detailinformationen zum Antragswesen können bei Bedarf von der GS-ITR 4.3 erfragt werden.

4. Betriebliche Anforderungen an den Zertifikats-Life-Cycle

Im folgenden Abschnitt werden die grundsätzlichen Parameter der Commerzbank Personen PKI aufgezeigt. Die Personen PKI dient der Ausgabe und Verwaltung von Benutzer- als auch von Zertifikaten für Commerzbank Gruppenpostfächer.

Zertifikatsantrag für Commerzbank Smart Card Benutzerzertifikate:

Die Erst-Beantragung und die Verlängerung von Smart Cardzertifikate für Commerzbank Benutzer erfolgt kontrolliert durch ein Zertifikats- und Smart Card Management Tool. Benutzerbezogene Zertifikate werden auf einer Smart Card provisioniert. Hierbei unterliegt die Zertifikatslebens-zyklusverwaltung und respektive die Smart Card Verwaltung der Kontrolle des Managementsystems.

Zertifikatsantrag für Commerzbank Gruppenpostfächer:

Die Erst-Beantragung und die Verlängerung von Zertifikaten für Commerzbank Gruppenpostfächern erfolgt kontrolliert durch ein Zertifikatsmanagement Tool. Hierbei unterliegt die Zertifikatslebenszyklusverwaltung der Kontrolle des Managementsystems.

Nutzung von Commerzbank Smart Card Benutzerzertifikaten:

Die Nutzung von Commerzbank Smart Card Zertifikaten erstreckt sich neben der Authentifikation, auch zur Verschlüsselung und zum Erstellen einer digitalen Signatur.

Detaillierte Anwendungsfälle können aus den Commerzbank Zertifikatsprofilen entnommen werden.

Folgende technische Rahmenbedingungen sind hervorzuheben:

- Benutzerzertifikate liegen auf der Smart Card/Chipkarte vor
- Die Verwaltung und Ausgabe von Commerzbank Smart Card Benutzerzertifikaten obliegt der Kontrolle durch das zentrale Zertifikatsmanagement Tool
- Zugehörige CPS, CRL und CA-Zertifikate sind veröffentlicht. Dies ermöglicht eine problemlose Kommunikation.
- SMIME eMail Zertifikate werden im Commerzbank Verzeichnisdienst veröffentlicht.
- Eine Schlüsselarchivierung von Verschlüsselungsschlüsseln ist etabliert

Weitergehende Informationen zum Einsatzbereich der Personen PKI können bei Bedarf von der GS-ITR 4.3 erfragt werden.

Nutzung von Zertifikaten für Commerzbank Gruppenpostfächer:

Die Nutzung des Zertifikats dient ausschließlich der Verschlüsselung von eMails für Gruppenpostfächer. Weitere Verwendungen sind ausgeschlossen.

Folgende technische Rahmenbedingungen sind hervorzuheben:

- Zertifikate für Gruppenpostfächer liegen nur als Software Zertifikate vor (Soft PSE)
- Die Verwaltung und Ausgabe von Zertifikaten für Gruppenpostfächer obliegt der Kontrolle durch das zentrale Zertifikatsmanagement Tool
- Zugehörige CPS, CRL und CA-Zertifikate sind veröffentlicht. Dies ermöglicht eine problemlose Kommunikation.
- Zertifikate für Gruppenpostfächer werden im Commerzbank Verzeichnisdienst veröffentlicht.
- Eine Schlüsselarchivierung von Verschlüsselungsschlüsseln für Gruppenpostfächer ist etabliert

Weitergehende Informationen zum Einsatzbereich der Personen PKI können bei Bedarf von der GS-ITR 4.3 erfragt werden.

4.1. Zertifikatsantrag

Im vorangegangenen Abschnitt 4. unter Beantragung und Nutzung ist der Prozess für den Zertifikatsantrag zu entnehmen. Weitergehende Informationen zum Zertifikatsantrag können bei Bedarf von der GS-ITR 4.3 erfragt werden.

4.1.1. Antragsberechtigt für ein Zertifikat

Antragsberechtigt für ein Zertifikat sind:

- alle Commerzbank Mitarbeiter,
- externe Mitarbeiter der längere Zeit bei der Commerzbank beschäftigt ist. Hierbei werden Smart Cards für Externe temporär ausgegeben.

4.1.2. Ausgabeprozess und Verantwortlichkeiten

Die Ausgabe von Smart Cards und Zertifikate für Gruppenpostfächer erfolgt durch die Commerzbank Personen PKI. Die Verantwortlichkeit für den Ausgabeprozess obliegen der GS-ITR 4.3. Eine detaillierte Beschreibung des Ausgabeprozess und technische Umsetzung kann bei Bedarf von der GS-ITR 4.3 erfragt werden.

4.2. Prozess für die Antragsbearbeitung

Wie auch beim Zertifikatsantrag ist die Antragsbearbeitung von Smart Card Zertifikaten und Zertifikate für Gruppenpostfächern ein kontrollierter Prozess durch das Zertifikatsmanagementsystem. Detailinformationen zur Antragsbearbeitung können bei Bedarf von der GS-ITR 4.3 erfragt werden.

4.2.1. Durchführung der Identifikation und Authentifizierung

Die Identifikation und Authentifizierung des Antragsstellers erfolgt auf Basis valider Commerzbank Domänenkonten. Dies gilt sowohl für die Beantragung von Smart Cards, als auch für die Beantragung von Zertifikaten für Commerzbank Gruppenpostfächern.

4.2.2. Annahme oder Ablehnung von Zertifikatsanträgen

Annahme oder Ablehnung des Antragsstellers erfolgt auf Basis valider Commerzbank Domänenkonten. Dies gilt sowohl für die Beantragung von Smart Cards, als auch für die Beantragung von Zertifikaten für Commerzbank Gruppenpostfächern.

4.2.3. Bearbeitungsdauer von Zertifikatsanträgen

Die Bearbeitung der Zertifikatsanträge für Benutzer und für Gruppenpostfächer erfolgt kontrolliert durch das Zertifikatsmanagementsystem. Dieses Verfahren erlaubt eine sofortige Ausstellung des Zertifikats an den Antragssteller.

In beiden o. g. Anwendungsfällen ergibt sich daraus eine sofortige Bearbeitung. Vorgelagerte Prozesse sind hierbei nicht berücksichtigt, was die Bearbeitungsdauer verlängern kann.

4.3. Zertifikatsausgabe

Wie auch beim Zertifikatsantrag ist die Zertifikatsausgabe von Benutzerzertifikaten und von Zertifikaten für Gruppenpostfächer ein kontrollierter Prozess durch das Zertifikatsmanagementsystem.

Weitergehende Informationen zur Zertifikatsausgabe können bei Bedarf erfragt werden. Die Detailverfahren zur Zertifikatsausgabe von Benutzerzertifikaten sind aus den Prozessabläufen für die Ausgabe von Smart Cards zu entnehmen.

4.3.1. Aktivitäten der CA bei Zertifikatsausgabe

Vor Ausgabe der Zertifikate an die Zertifikatsnehmer werden folgende Arbeitsschritte CA-seitig ausgeführt.

- Validierung der Zertifikatsanforderung für durch das CA Richtlinienmodul
    - Bei kontrollierter Ausgabe durch das Zertifikatsmanagementsystem erfolgt die Validierung durch das Zertifikatsmanagement Richtlinienmodul.
- Archivierung der ausgegebenen Zertifikate und Zertifikatsanforderungen in der Datenbank der Commerzbank AG Inhouse Sub CA 03.
- Archivierung der ausgegebenen Zertifikatsinformationen und des Antragsablaufs in der Datenbank des Zertifikatsmanagementsystems. Darüber hinaus werden Smart Card-relevante Informationen, wie die PUK (Admin Key), als auch Zusatzinformationen in dieser Datenbank verschlüsselt abgelegt.
- Beim Einsatz von Verschlüsselungsschlüsseln für Benutzer werden diese in der Datenbank der Commerzbank AG Inhouse Sub CA 03 archiviert.
- Die Ausgabe der Zertifikate für den Antragssteller erfolgt kontrolliert über das Zertifikatsmanagementsystem.

4.3.2. Ausgabebenachrichtigung der Zertifikatsnehmer durch die CA

Eine Ausgabebenachrichtigung durch die ausstellende Zertifizierungsstelle und zusätzlich durch das Commerzbank Trustcenter findet statt.

4.4. Zertifikatsannahme

Wie auch beim Zertifikatsantrag ist die Zertifikatsannahme von Benutzerzertifikaten und Zertifikate für Gruppenpostfächer ein kontrollierter Prozess durch das Commerzbank Zertifikatsmanagementsystem.

Die Detailverfahren zur Zertifikatsannahme von Benutzerzertifikaten sind aus den Prozessabläufen für die Ausgabe von Smart Cards zu entnehmen und können bei Bedarf bei GS-ITR 4.3 erfragt werden.

4.4.1. Verfahren der Zertifikatsannahme

Die Zertifikatsannahme findet wie auch schon bei der Antragsstellung durch die Personen PKI statt.

- Im Falle von Zertifikaten für Gruppenpostfächer gilt: Wenn das Zertifikatsmanagement-system den Ausgabeprozess als „abgeschlossen“ protokolliert hat.
- Im Falle von Benutzerzertifikaten für Smart Cards gilt: Wenn das Zertifikatsmanagement-system den Ausgabeprozess als „abgeschlossen“ protokolliert hat.

4.4.2. Publikation des Zertifikats

Die Publikation der Verschlüsselungszertifikate erfolgt automatisiert durch die Personen PKI in den lokalen Verzeichnisdienst. Keine Benutzerintervention ist hierzu notwendig.

Die Publikation der Commerzbank CA Zertifikate für die Commerzbank AG Inhouse Root CA und die Commerzbank AG Inhouse Sub CA 03 wird auf den PKI Web Servern manuell durch die GS-ITR 4.3 ausgeführt. Dies gilt auch für die Erneuerung der o. g. CA Zertifikaten.

4.4.3. Ausgabebenachrichtigung anderer Entitäten durch die CA

Eine Ausgabebenachrichtigung an andere Entitäten durch die Commerzbank CAs findet nicht statt.

4.5. Schlüsselpaar- und Zertifikatsverwendung

Grundsätzlich ist der Gebrauch des Schlüsselpaares für die Authentifikation und zur Verschlüsselung/Entschlüsselung von Informationen und zur Erstellung /Validierung von Signaturen vorgesehen.

4.5.1. Nutzung des privaten Schlüssels und Zertifikats durch den Zertifikatsnehmer

Die Nutzung der Zertifikate durch den Zertifikatsnehmer hat den Commerzbank Zertifikatsrichtlinien zu folgen. In Kapitel 1.4. Anwendungsbereich von Zertifikaten sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt. Außerdem muss der Zertifikatsnehmer bei der Nutzung der privaten Schlüssel seine in der Commerzbank Policy für Smart Cards definierten Pflichten erfüllen.

4.5.2. Nutzung des privaten Schlüssels und Zertifikats durch vertrauende Parteien

Die Nutzung der Zertifikate durch vertrauende Parteien hat den zugewiesenen Zertifikatsrichtlinien seiner Organisation zu folgen. Dort sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt.

4.6. Zertifikatserneuerung

In Rahmen der Commerzbank Personen PKI findet die Zertifikatserneuerung ausschließlich mit Schlüsselwechsel statt. Eine Erneuerung der Zertifikatslebensdauer mit gleichbleibenden Schlüsselpaaren ist nicht vorgesehen. Daher sind alle nachfolgenden Punkte unter 4.6. für die Commerzbank Personen PKI nicht zutreffend.

4.6.1. Umstände für eine Zertifikatserneuerung

Nicht zutreffend.

4.6.2. Antragsberechtigte für eine Zertifikatserneuerung

Nicht zutreffend.

4.6.3. Durchführen einer Zertifikatserneuerung

Nicht zutreffend.

4.6.4. Erneuerungsbenachrichtigung für den Zertifikatsnehmer

Nicht zutreffend.

4.6.5. Verfahren zur Annahme der Zertifikatserneuerung

Nicht zutreffend.

4.6.6. Publikation des erneuerten Zertifikats durch die CA

Nicht zutreffend.

4.6.7. Erneuerungsbenachrichtigung anderer Entitäten durch die CA

Nicht zutreffend.

4.7. Zertifikatserneuerung mit Schlüsselwechsel

In Rahmen der Commerzbank Personen PKI findet die Zertifikatserneuerung nur ausschließlich mit Schlüsselwechsel statt. Eine Anpassung der Zertifikatsinhalte (Datenanpassung) ist vorgesehen, da sich Personendaten wie E-Mail Adresse und Namen über die Laufzeit hin sich verändern können. Alle nachfolgenden Punkte unter 4.7. für die Commerzbank Personen PKI nicht zutreffend.

4.7.1. Umstände für eine Zertifikatserneuerung mit Schlüsselwechsel

Nicht zutreffend.

4.7.2. Antragsberechtigte für eine Zertifikatserneuerung mit Schlüsselwechsel

Nicht zutreffend.

4.7.3. Durchführen einer Zertifikatserneuerung mit Schlüsselwechsel

Nicht zutreffend.

4.7.4. Erneuerungsbenachrichtigung für den Zertifikatsnehmer

Nicht zutreffend.

4.7.5. Verfahren zur Annahme der Zertifikatserneuerung mit Schlüsselwechsel

Nicht zutreffend.

4.7.6. Publikation des erneuerten Zertifikats durch die CA

Nicht zutreffend.

4.7.7. Erneuerungsbenachrichtigung anderer Entitäten durch die CA

Nicht zutreffend.

4.8. Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

In Rahmen der Commerzbank Personen PKI findet die Zertifikatserneuerung ausschließlich mit Schlüsselwechsel statt. Technisch betrachtet handelt es sich um die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer und für einen neuen öffentlichen Schlüssel (respektive auch neuen privaten Schlüssel) und möglicher Anpassung von Inhaltsdaten.

4.8.1. Umstände für eine Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Die Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung kann beantragt werden, wenn die folgenden Voraussetzungen erfüllt sind:

- die Gültigkeitsdauer des aktuellen Zertifikats ist abgelaufen oder steht kurz vor Ablauf
- das alte Zertifikat wurde gesperrt
- die im Zertifikat enthaltenen Daten sind nicht korrekt.
- der alte Schlüssel kann oder darf nicht mehr verwendet werden, weil er (möglicherweise) kompromittiert wurde
- die Gültigkeitsdauer des aktuellen Zertifikats oder die aktuelle Schlüssellänge bietet keine ausreichende Sicherheit mehr
- kann technisch nicht mehr genutzt werden kann (Verlust des privaten Schlüssels oder kein Zugriff auf private Schlüssel)

4.8.2. Antragsberechtigte für eine Zertifikatserneuerung mit Schlüsselwechsel

Sind alle Zertifikatsnehmer, denen ein gültiges Zertifikat durch die Personen PKI zugewiesen wurde und:

- Commerzbank Mitarbeiter,
- externe Mitarbeiter der längere Zeit bei der Commerzbank beschäftigt ist. Hierbei werden Smart Cards für Externe temporär ausgegeben

4.8.3. Durchführen einer Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Der Prozess erfolgt analog der Erst-Antragsstellung. Die Commerzbank Personen PKI führt die Zertifikatserneuerung mit Schlüsselwechsel von Benutzerzertifikaten für Smart Cards und Zertifikate für Gruppenpostfächer kontrolliert durch das Zertifikats- und Smart Card Managementsystem.

4.8.4. Erneuerungsbenachrichtigung für den Zertifikatsnehmer

Bei der kontrollierten Ausgabe- und Erneuerung durch das Zertifikats- und Smart Card Managementsystem wird eine Erneuerungsbenachrichtigung an den Antragssteller per eMail versendet. Die Erneuerungsbenachrichtigung wird an die Beteiligten innerhalb des Erneuerungsintervalls versandt.

4.8.5. Verfahren zur Annahme der Zertifikatserneuerung mit Schlüsselwechsel mit Datenanpassung

Die Zertifikatsannahme findet wie auch schon bei der Antragsstellung durch die Personen PKI statt.

- Im Falle von Zertifikaten für Gruppenpostfächer gilt: Wenn das Zertifikatsmanagement-system den Ausgabeprozess als „abgeschlossen“ protokolliert hat.
- Im Falle von Benutzerzertifikaten für Smart Cards gilt: Wenn das Zertifikatsmanagement-system den Ausgabeprozess als „abgeschlossen“ protokolliert hat.

4.8.6. Publikation des erneuerten Zertifikats durch die CA

Die Publikation der Verschlüsselungszertifikate erfolgt automatisiert durch die Personen PKI in den lokalen Verzeichnisdienst. Keine Benutzerintervention ist hierzu notwendig.

Die Publikation der Commerzbank CA Zertifikate für die Commerzbank AG Inhouse Root CA und die Commerzbank AG Inhouse Sub CA 03 wird auf den PKI Web Servern manuell durch die GS-ITR 4.3 ausgeführt.

4.8.7. Erneuerungsbenachrichtigung anderer Entitäten durch die CA

Eine Ausgabebenachrichtigung an andere Entitäten durch die Commerzbank CAs findet nicht statt.

4.9. Zertifikatssperrung und -suspendierung

Es ist primär eine Zertifikatssperrung und keine Zertifikatssuspendierung vorgesehen. Weitergehende Informationen zur Zertifikatssperrung können bei Bedarf von der GS-ITR 4.3 erfragt werden.

4.9.1. Umstände für die Sperrung

Eine Zertifikatssperrung ist in den folgenden Fällen zu sperren:

- Wenn die Commerzbank Benutzer Smart Card entwendet, beschädigt oder verloren wurde, d. h. eine permanente Ersatzkarte mit neuen Zertifikaten ausgestellt wird.
- Wenn der berechtigte Verdacht besteht, dass der private Schlüssel, der zum öffentlichen Schlüssel im Zertifikat korrespondiert, kompromittiert wurde, d.h. dass ein Unbefugter den privaten Schlüssel nutzen kann.

- Wenn der berechtigte Verdacht besteht, dass die für die Erzeugung und Anwendung des privaten Schlüssels, der zum öffentlichen Schlüssel im Zertifikat korrespondiert, eingesetzten Algorithmen, Parameter und Geräte die Fälschungssicherheit der erzeugten Signaturen nicht mehr gewährleisten.
- Wenn der Eigentümer sein Zertifikat nicht mehr nutzen kann, z.B. der Benutzer keinen Zugriff auf das Schlüsselmaterial mehr hat.
- Wenn zu dem Zertifikat, eine Zertifikatserneuerung mit Schlüsselwechsel beantragt wurde oder in Kürze beantragt wird.
- Wenn die Commerzbank AG ihre Zertifizierungsdienste eingestellt. In diesem Fall werden sämtliche von den Zertifizierungsdiensten ausgestellten Zertifikate gesperrt.
- Wenn der Zertifikatseigentümer die Voraussetzungen für die Beantragung des Zertifikates nicht mehr erfüllt, z.B. weil der Commerzbank Mitarbeiter aus dem Dienst ausscheidet oder gegen die bestehende Zertifikatsrichtlinie verstoßen wird.

4.9.2. Antragsberechtigte für eine Sperrung

Folgende Personenkreise und Instanzen sind berechtigt Zertifikate zu sperren:

- die Sperrung eines Zertifikats kann durch
  - den Zertifikatsnehmer selbst (Zertifikatsinhaber),
  - seinen Vertreter (durch Vollmacht),
  - seinen Vorgesetzten oder
- Die Sperrung von CA Zertifikaten kann durch die Commerzbank RA Officer veranlasst werden.

4.9.3. Durchführung einer Zertifikatssperrung

Die Zertifikatssperrung erfolgt per eMail oder telefonisch. Die Identifikation des Antragsberechtigten wird mit geeigneten Mitteln ausgeführt.

Durchgeführt wird die Zertifikatssperrung grundsätzlich durch die Commerzbank RA Officer oder den LROs. Hierzu wird die Sperrung mit Hilfe des Zertifikats- und Smart Card Managementsystem der Commerzbank Personen PKI ausgeführt.

4.9.4. Meldefrist von Sperranträgen für Zertifikatsnehmer

Es sind keine vorgeschriebenen Fristen festgelegt. Grundsätzlich soll eine Meldung von Sperranträgen direkt erfolgen.

4.9.5. Bearbeitungsdauer von Sperranträgen durch die CA

Es ist keine festgeschriebene Bearbeitungsdauer von Sperranträgen durch die CA spezifiziert.

4.9.6. Prüfung des Zertifikatsstatus durch vertrauende Parteien

Eine Überprüfung des Zertifikatsstatus durch vertrauende Parteien wird empfohlen. Der Sperrstatus von Commerzbank Zertifikaten und von Commerzbank Zertifizierungsstellen Zertifikaten können über die entsprechenden Sperrlisten geprüft werden. Die aktuellen Zertifikatssperrlisten können durch die in den Zertifikat enthaltenen CDPs (CRL Distribution Points) heruntergeladen werden.

4.9.7. Ausstellungszeiträume für CRLs

Folgende Ausgabeschemata sind für die Commerzbank Personen PKI gültig:

Commerzbank Inhouse Root CA:

- CRL Veröffentlichungsperiode: 3 Monate
- CRL Veröffentlichung Überlappungsperiode: 1 Monat

Commerzbank Inhouse Sub CA 03:

- CRL Veröffentlichungsperiode: 1 Woche
- CRL Veröffentlichung Überlappungsperiode: 1 Woche

4.9.8. Maximale Latenz von CRLs

- Die CRLs stehen sofort nach Veröffentlichung auf den Commerzbank PKI Web-Servern zur Verfügung. Eine Latenzzeit von CRLs ist daher nicht zu erwarten.

4.9.9. Online Sperrung und Statusprüfung von Zertifikaten

nicht zutreffend. Online Sperrung und Statusprüfung ist für die Commerzbank Personen PKI nicht vorgesehen.

4.9.10. Anforderung für die Online Prüfung des Sperrstatus

nicht zutreffend.

4.9.11. Weitere Arten zur Bekanntmachung von Zertifikatsstatus

Keine weiteren. Commerzbank CRLs werden auf Web-Servern Lokation veröffentlicht, welche im Zertifikat über die CDP Einträge bekannt gemacht werden.

4.9.12. Spezielle Maßnahmen bei Schlüsselkompromittierung

Bei einem Hinweis einer Schlüsselkompromittierung wird eine entsprechende Untersuchung durchgeführt. Sollte die Kompromittierung sich als stichhaltig erweisen, so werden die notwendigen Maßnahmen ergriffen, wie die Sperrung der betroffenen Zertifikate.

4.9.13. Umstände für eine Suspendierung

Nicht zutreffend, da eine komplette Sperrung des Zertifikats vorgesehen ist.

4.9.14. Berechtigte für eine Suspendierung

Nicht zutreffend, da eine komplette Sperrung des Zertifikats vorgesehen ist.

4.9.15. Durchführung einer Suspendierung

Nicht zutreffend, da eine komplette Sperrung des Zertifikats vorgesehen ist.

4.9.16. Dauer einer Suspendierung

Nicht zutreffend, da eine komplette Sperrung des Zertifikats vorgesehen ist.

4.10. Auskunftsdienste für den Zertifikatsstatus

Die Commerzbank AG betreibt einen Auskunftsdienst über den Zertifikatsstatus. Dieser Auskunftsdienst ist web-basiert und wird durch die URL http://ca.commerzbank.com/cdp/ repräsentiert. Es werden die CRLs (Zertifikatssperrlisten) veröffentlicht:

- Die Statusinformationen zu den End-Entitäten Zertifikaten werden in der CRL durch die Commerzbank AG Inhouse Sub CA 03 veröffentlicht.
- Die Statusinformationen zu den Zertifikaten der Zertifizierungsstellen werden in der CRL, ausgegeben durch die Commerzbank AG Inhouse Root CA, veröffentlicht.

Für jeden dieser Zertifikatstypen werden separate CRLs (Sperrlisten) veröffentlicht.

4.10.1. Betriebliche Ausprägung

Der Auskunftsdienst ist web basierend und verwendet als Übertragungsprotokoll http.

Auf folgenden URLs können die CRLs der Root CA bzw. Sub CA 03 abgerufen werden:

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

Die CRLs und zu sperrende Zertifikate müssen von der gleichen Zertifizierungsstelle ausgegeben worden sein. Eine Unterstützung von „indirekten CRLs“ ist in der jetzigen Implementierung nicht gegeben.

Das ausgegebene CRL Profil ist zu RFC 5280 konform und entspricht dem X.509 Version 2 Standard.

4.10.2. Verfügbarkeit des Auskunftsdienstes

Die Verfügbarkeit der Commerzbank PKI Web-Server ist für einen 7 x 24h Betrieb ausgelegt.

4.10.3. Optionale Funktionen

Keine.

4.11. Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer

Ein Eigentümer oder Zertifikatsnehmer eines Commerzbank Zertifikats scheidet aus den Zertifizierungsdiensten aus, wenn er aus dem Arbeitsverhältnis der Commerzbank AG ausscheidet bzw. sein Arbeitsverhältnis als externer Mitarbeiter endet.

4.12. Schlüsselhinterlegung und -wiederherstellung

Eine Schlüsselhinterlegung und –wiederherstellung wird in Rahmen der Commerzbank Personen PKI für Verschlüsselungsschlüssel praktiziert.

Für die Wiederherstellung von Benutzerschlüssel wird auf eine Sicherungskopie der Schlüssel zurückgegriffen. Die Umsetzung wird durch das Smart Card Managementsystem und der zugehörigen Zertifizierungsstelle Commerzbank AG Inhouse Sub CA 03 ausgeführt, welche das Schlüsselmaterial des Benutzers verschlüsselt in der CA Datenbank archiviert. Eine Detailbeschreibung dieses Prozesses kann von der GS-ITR 4.3 erfragt werden.

4.12.1. Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

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

4.12.2. Richtlinien und Praktiken zur Hinterlegung und Wiederherstellung von Sitzungsschlüsseln (symmetrischen Schlüsseln)

Nicht zutreffend. Sitzungsschlüssel werden nicht archiviert.

5. Einrichtungen, Sicherheitsmanagement, organisatorische und betriebliche Sicherheitsmassnahmen

5.1. Physikalische- und Umgebungssicherheit

Die infrastrukturellen Sicherheitsmaßnahmen der Commerzbank Personen PKI sind in den Commerzbank AG Rechenzentrumsbetrieb eingebettet. Nachfolgende Vorkehrungen und physikalische Schutzmaßnahmen sind integraler Bestandteil der Rechenzentren betrieben durch die Commerzbank AG.

5.1.1. Lage und Konstruktion

Die Systeme der Commerzbank Personen PKI befinden sich in den Räumlichkeiten der Commerzbank Rechenzentren. Die Räume bieten hinsichtlich der physikalischen Sicherheitsmaßnahmen einen ausreichenden Schutz, der dem erforderlichen Sicherheitsniveau angemessen ist.

5.1.2. Zutrittskontrolle

Die Betriebsräume der Zertifizierungsstellen sind durch geeignete technische und infrastrukturelle Maßnahmen gesichert. Ein Zutritt zu den Betriebsräumen der Zertifizierungsstelle wird nur Mitarbeitern gestattet, die die entsprechende Freigabestufe besitzen. Der Zutritt durch betriebsfremde Personen wird durch eine Besucherregelung festgelegt.

5.1.3. Stromversorgung und Klimatisierung

Die Installation zur Stromversorgung entspricht den erforderlichen Normen, eine Klimatisierung der Räume für die technische Infrastruktur ist vorhanden.

5.1.4. Wasserschäden

Die Räume für die technische Infrastruktur verfügen über einen angemessenen Schutz vor Wasserschäden.

5.1.5. Prävention und Schutz vor Feuer

Die bestehenden Brandschutzvorschriften werden eingehalten.

5.1.6. Datenträger

Es werden folgende Datenträger verwendet:

- Papier
- CD-ROMs
- USB-Speichermodule
- Magnetbänder
- Hardwaretoken

Datenträger werden in verschlossenen Schränken aufbewahrt. Datenträger mit sensiblen Daten, wie z. B. HSM Hardware Tokens, werden in einem Tresor aufbewahrt.

5.1.7. Abfall Entsorgung

Informationen auf elektronischen Datenträgern werden sachgemäß vernichtet und anschließend sachgerecht entsorgt. Papierdatenträger werden mittels vorhandenen Aktenvernichtern zerstört und auch hier sachgerecht entsorgt.

5.1.8. Off-site Backup

Der Commerzbank Rechenzentrumsbetrieb regelt die Anlage von Off-Site Sicherungen.

5.2. Organisatorische Sicherheitskontrollen

5.2.1. Sicherheitskritische Rollen

Sicherheitskritische Aufgaben werden für den Betrieb der Commerzbank Personen PKI in Rollen zusammengefasst. Ein PKI Rollenkonzept ist verfügbar und wird für den organisatorischen Prozess und auch für den HSM (Hardware Security Module) Betrieb umgesetzt.

Eine Beschreibung der Rollendefinition kann bei Bedarf von der GS-ITR 4.3 erfragt werden.

5.2.2. Zugewiesene Zahl von Personen bei sicherheitskritischen Aufgaben

Das Vier-Augen-Prinzip gilt bei folgenden Operationen:

- Wiederherstellen des Schlüsselmaterials der Commerzbank Zertifizierungsstellen
- Wiederherstellen der Commerzbank Zertifizierungsstellen
- Zugriff auf die Hardware Security Module der Commerzbank Zertifizierungsstellen

5.2.3. Identifikation und Authentifikation der Rollen

Die Identifikation und Authentisierung der Benutzer erfolgt beim Zutritt zu sicherheitsrelevanten Räumen und beim Zugriff auf sicherheitsrelevante Systeme mit Hilfe von Smart Cards, Hardware Tokens und/oder Benutzername und Passwort.

Bei besonders sicherheitskritischen Operationen, wie die Verwaltung von Zertifizierungsstellen-schlüssel wird das Vier-Augen-Prinzip adressiert.

5.2.4. Trennung von Rollen und Aufgaben

Das Rollenkonzept regelt auch, welche Zuordnungen von Personen zu Rollen sich gegenseitig ausschließen. Detailinformationen zur Rollen- und Aufgabentrennung können bei GS-ITR 4.3 erfragt werden.

5.3. Sicherheitsmassnahmen für das Personal

Die Commerzbank AG stellt in Rahmen der Personen PKI erfahrenes Personal zur Verfügung. Notwendige Qualifikation, Wissenstand und Erfahrungswerte des Personals sind für den sicheren PKI Regelbetrieb vorhanden.

5.3.1. Anforderung an Qualifikation, Erfahrung und Freigabestufe

Das zuständige Personal verfügt über die erforderlichen spezifischen Kenntnisse und Erfahrungen aus dem Bereich der Personen PKI. Ebenso sind grundlegende IT Kenntnisse vorhanden um auch systemnahe Operationen auszuführen.

5.3.2. Prozess zur Sicherheitsüberprüfung von Mitarbeitern

Es gelten die allgemeinen Personaleinstellungsrichtlinien der Commerzbank AG.

5.3.3. Trainingsanforderung

Das für den Zertifizierungsdienst eingesetzte Personal wird vor Aufnahme der Tätigkeit ausreichend geschult. Das Training beinhaltet auch eine Sensibilisierung der Mitarbeiter hinsichtlich der Sicherheitsrelevanz ihrer Arbeit und potenzieller Bedrohungen.

5.3.4. Trainingsfrequenz

Die Frequenz der Trainings orientiert sich an den Anforderungen der Commerzbank Personen PKI. Trainings werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

5.3.5. Frequenz und Abfolge von Job Rotation

Eine Job Rotation ist nicht vorgesehen.

5.3.6. Sanktionen bei unzulässigen Handlungen

Die allgemeinen Sanktionsmöglichkeiten der Commerzbank AG werden bei unzulässigen Handlungen angewandt.

5.3.7. Vertragsbedingungen für das Personal

Das Commerzbank PKI Betriebspersonal verpflichtet sich auf die die Einhaltung von Anweisungen und gesetzlichen Vorschriften. Diese beinhalten insbesondere eine Verpflichtung, personenbezogene Daten vertraulich zu behandeln.

5.3.8. An das Personal ausgehändigte Dokumente

Folgende Dokumente werden dem Commerzbank Personal zum ordnungsgemäßen Betrieb der Personen PKI zur Verfügung gestellt:

- Zertifikatsrichtlinie oder Certificate Policy (CP)
- Erklärung zum Zertifizierungsbetrieb oder Certification Practice Statement (CPS)
- Betriebskonzept und Sicherheitskonzept des Personen PKIs
- Handlungsanweisungen
- Betriebshandbücher der Systeme und Software

5.4. Überwachung von sicherheitskritischen Ereignissen

5.4.1. Protokollierte Ereignisse

Zu jedem Ereignis werden folgenden Daten erfasst:

- Zeitpunkt (Datum und Uhrzeit)
- Log ID des Eintrages
- Art des Ereignisses
- Ursprung des Ereignisses

5.4.2. Überprüfungshäufigkeit von Log-Daten

Eine Überprüfung der Log-Daten sollte in regelmäßigen Abständen stattfinden. Bei Verdacht auf Unregelmäßigkeiten wird eine umgehende Prüfung veranlasst.

5.4.3. Aufbewahrungsfristen von Audit Log-Daten

Sicherheitsrelevante Protokolldaten werden entsprechend den gesetzlichen Regelungen aufbewahrt.

5.4.4. Schutzmassnahmen von Audit Log-Daten

Elektronische Log-Dateien werden mit Mitteln des Betriebssystems gegen Zugriff, Löschung und Manipulation geschützt und sind nur den System- und Netzwerkadministratoren zugänglich.

5.4.5. Audit Log-Daten Backup-Verfahren

Die Protokolldaten werden zusammen mit anderen relevanten Daten einem regelmäßigen Backup unterzogen. Protokolle auf Papier werden in verschließbaren Schränken verwahrt.

5.4.6. Audit Collection System (Protokollierungssystem intern oder extern)

Alle Protokoll-Dateien werden regelmäßig gesichert.

5.4.7. Benachrichtigung bei Auslösen eines sicherheitskritischen Ereignisses

Eine Benachrichtigung des PKI Bedienerpersonals findet bei Auftreten von Produktionsproblemen statt.

5.4.8. Schwachstellenanalyse

Nicht zutreffend.

5.5. Archivierung von Protokolldaten

Die Commerzbank AG archiviert in Rahmen des Personen PKI Betriebes die notwendigen Protokolldaten.

5.5.1. Archivierte Protokolldatentypen

Archiviert werden Daten, die für den Zertifizierungsprozess relevant sind:

- Zertifikatanträge, diese enthalten persönliche Daten des Zertifikatnehmers
- Alle von der Zertifizierungsstelle ausgestellten Zertifikate
- Sperranträge für Zertifikate und für Zertifizierungsstellen Zertifikate
- Vor einer Modifikation eines Systems gesicherte Systemdaten
- Datensicherungen der Produktivsysteme
- Dokumentation der personellen Sicherheitsmaßnahmen (z.B. Dienstpläne, Dokumentation der Sicherheitsüberprüfungen)
- Dokumentationen von Prozeduren und Systemen (z.B. Handlungsanweisungen, Notfallpläne, Systemhandbücher)
- Protokolle von sicherheitsrelevanten interner Prozeduren und Prozesse

5.5.2. Archivierungsfristen

Zu archivierende Daten werden gemäß den Commerzbank Regelungen aufbewahrt.

5.5.3. Schutzmaßnahmen für das Archiv

Es wird durch geeignete Maßnahmen sichergestellt, dass die Daten nicht verändert oder gelöscht werden können. Sind in den Archiven personenbezogene Daten enthalten, wird darüber hinaus sichergestellt, dass die Daten nicht unbefugt gelesen oder kopiert werden können.

Die Schutzmaßnahmen für elektronische Datenträger entsprechen den für den Rechenzentrums-Betriebs der Commerzbank AG vorgesehenen Prozessen.

5.5.4. Backup-Verfahren für das Archiv

Die Verfahren und Prozesse für das Archiv Backup folgt der für den Rechenzentrumsbetrieb der Commerzbank AG vorgesehenen Umsetzung.

5.5.5. Zeitstempelanforderungen für archivierte Daten

Audit Logs, protokollierte Ereignisse, archivierte Daten, Zertifikate, Zertifikatssperrlisten und andere Eintragungen enthalten jeweils eine eindeutige Zeit- und Datumsangabe. Datums- und Zeitangaben von Online-Systemen werden in regelmäßigen Abständen gegen eine vertrauenswürdige Zeitquelle synchronisiert.

5.5.6. Archivierungssystem (intern oder extern)

Ein Archivierungssystem wird in Rahmen der Commerzbank Personen PKI eingesetzt.

5.5.7. Verfahren zur Beschaffung und Verifizierung von Archivdaten

Das Commerzbank AG Personen PKI Betriebskonzept beschreibt die Prozesse für die Beantragung und Verifikation von Archivdaten. Eine Detailbeschreibung dieses Prozesses kann von der GS-ITR 4.3 erfragt werden.

5.6. Schlüsselwechsel der Zertifizierungsstellen

Bei einem Schlüsselwechsel der Commerzbank AG Inhouse Root CA wird das alte CA Zertifikat zerstört und ein neues selbst-signiertes Zertifikat ausgestellt und veröffentlicht. Eine Sperrung der selbst-signierenden Root CA Zertifikats ist technisch auf der CA Seite nicht machbar.

Bei einem Schlüsselwechsel der Commerzbank AG Inhouse Sub CA 03 für Benutzerzertifikate wird das Inhouse Sub CA 03 Zertifikat von der Commerzbank AG Inhouse Root CA gesperrt und eine neues Zertifikat ausgestellt und veröffentlicht. Die Beantragung selbst erfolgt durch die Commerzbank AG Inhouse Sub CA 03.

Die CA Zertifikatserneuerung mit Schlüsselwechsel folgt unten aufgeführtem Schema:

Commerzbank AG Inhouse Root CA

- Root CA Zertifikat: 30 Jahre
- Root CA CRLs: 4 Monate
- Erneuerungsperiode Commerzbank AG Inhouse Root CA Zertifikat spätestens 12 Monate vor Ablauf

Commerzbank AG Inhouse Sub CA 03

- Sub CA 03 Zertifikat: 10 Jahre
- Sub CA 03 CRLs: 12 Tage
- Erneuerungsperiode Commerzbank AG Inhouse Sub CA 03 Zertifikat spätestens 6 Monate vor Ablauf

5.7. Kompromittierung und Wiederanlauf nach Katastrophen

5.7.1. Prozeduren bei Sicherheitsvorfällen und Kompromittierung

Es existieren Notfallpläne der Commerzbank AG, in denen die Prozesse, Prozeduren und Verantwortlichkeiten bei Notfällen und Katastrophen geregelt sind. Zielsetzung dieser Notfall - Prozeduren ist die Minimierung von Ausfällen der Zertifizierungsdienstleistungen bei gleichzeitiger Aufrechterhaltung der Sicherheit. Die Notfall-Prozeduren sehen bei Sicherheitsvorfällen insbesondere die folgenden Maßnahmen vor:

- Analyse und Bewertung der Funktionseinschränkung und Sicherheitsprobleme der betroffenen Dienste und Systeme der Zertifizierungsstelle
- Festlegung von Sofortmaßnahmen, die den Funktionseinschränkungen und Sicherheitsproblemen entgegenwirken
- Regelung der Verantwortlichkeiten und Rollen
- Falls erforderlich, Benachrichtigung betroffener Stellen und Personen, z.B. der Zertifikatsnehmer, über die Problematik und gegebenenfalls notwendige Gegenmaßnahmen
- Analyse und Dokumentation der Ursachen des Vorfalles
- Gegebenenfalls Erstellung, Prüfung und Genehmigung eines Change Requests zur Modifikation der Systemkonfiguration mit dem Ziel, Vorfälle dieser Art in Zukunft zu verhindern. Überwachung der Umsetzung des Change Requests
- Protokollierung der einzelnen Maßnahmen und Tätigkeiten

5.7.2. Kompromittierung bei IT Ressourcen

Werden innerhalb der Zertifizierungsstelle fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der Zertifizierungsstelle haben,

- wird der Betrieb des entsprechenden IT-Systems unverzüglich eingestellt.
- Das IT-System wird neu aufgesetzt unter Wiederherstellung der Software und der Daten aus der Datensicherung, überprüft und in einem sicheren Zustand in Betrieb genommen.
- Anschließend wird das fehlerhafte oder modifizierte IT-System analysiert. Bei Verdacht einer vorsätzlichen Handlung werden gegebenenfalls rechtliche Schritte eingeleitet.
- Falls sich in einem Zertifikat fehlerhafte Angaben befinden, wird der Zertifikatnehmer unverzüglich informiert und das Zertifikat widerrufen.

5.7.3. Wiederanlauf bei Kompromittierung von privaten Schlüsselmaterial

Die Kompromittierung von privatem Schlüsselmaterial stellt einen ernstzunehmenden Zwischenfall und wird daher besonders gehandhabt.

- Bei Kompromittierung von privatem Schlüsselmaterial der Zertifizierungsstellen wird das jeweilige Zertifikat sofort gesperrt. Gleichzeitig werden alle mit Hilfe dieses Zertifikats ausgestellten Zertifikate gesperrt.
- Bei Kompromittierung von privatem Schlüsselmaterial des Commerzbank Benutzerzertifikats für Smart Cards und Zertifikate für Gruppenpostfächer wird das jeweilige Zertifikat sofort gesperrt.
- Sofern der Verdacht besteht, dass die für die Erzeugung und Anwendung des privaten Schlüssels eingesetzten Algorithmen, Parameter oder Geräte unsicher sind, wird eine entsprechende Untersuchung durchgeführt.
- Alle betroffenen Zertifikatsnehmer und vertrauende Parteien werden umgehend benachrichtigt.

5.7.4. Notfallbetrieb nach einem Katastrophenfall

Eine Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe bei Verlust ist Bestandteil der Notfallplanung und kann innerhalb kurzer Zeit erfolgen, sofern die Sicherheit der Zertifizierungsdienstleistung gegeben ist.

5.7.5. Einstellung des Betriebs der Zertifizierungs- und/oder Registrierungsstelle

Im Falle der Einstellung des Betriebes der Commerzbank AG Zertifizierungsstellen oder der Registrierungsstellen sind folgende Maßnahmen festgelegt:

- Alle Zertifikatsnehmer und vertrauende Parteien werden von der Einstellung des Zertifizierungsdienstes informiert. Eine zeitliche Frist wurde noch nicht festgelegt.
- Alle Benutzerzertifikate, sowie die Zertifikate der Zertifizierungsstellen werden gesperrt.
- Alle privaten Schlüssel der Zertifizierungsstellen und Benutzerzertifikate für Smart Cards der Zertifikatsnehmer werden vernichtet.
- Ausnahme bildet das Schlüsselmaterial für die Verschlüsselung. Diese werden in gesicherten Umgebungen, z. B. verschlüsselte Datenbank, archiviert.

6. Technische Sicherheitsmaßnahmen

6.1. Schlüsselpaarerzeugung und Installation

6.1.1. Schlüsselpaarerzeugung

Die Schlüsselerzeugung und die Auswahl der Crypto-Algorithmen für die Commerzbank Personen PKI erfolgt nach FIPS 140-2 Level 1 bzw. 3 (Federal Information Processing Standards).

Die Generierung der Schlüsselpaare wird von Hard- und Softwarekomponenten ausgeführt und unterscheidet sich je nach Entität:

Schlüsselpaargenerierung für die Commerzbank Zertifizierungsstellen:

Alle Schlüsselpaare für die Commerzbank Zertifizierungsstellen werden durch das Netzwerk-HSM (Hardware Security Modul) generiert. Die generierten CA Schlüssel werden auch durch das Netzwerk HSM kryptographisch geschützt. Jeglicher Prozess, der den Zugriff auf den privaten Schlüssel der Zertifizierungsstelle erforderlich macht, ist das HSM zwingend eingebunden. Die Commerzbank Netzwerk HSM wird im Fips 140-2 Level 3 Modus betrieben.

Schlüsselpaargenerierung der Schlüssel für Commerzbank Gruppenpostfach Zertifikate:

Die Schlüsselpaare für die Commerzbank Gruppenpostfächerwerden durch das Personen PKI für den Commerzbank Zertifikatsnehmer generiert. Die Generierung des Schlüsselmaterials erfolgt in diesem Fall durch Softwarekomponenten. Die Software Crypto-Komponenten sind nach FIPS 140-2 Level 1 zertifiziert.

Schlüsselpaargenerierung der Schlüssel für Commerzbank Benutzerzertifikate auf Smart Cards:

Das Authentifikations- und Signaturschlüsselpaar für Benutzerzertifikate auf Smart Cards wird durch die eingesetzte Smart Card für den Commerzbank Zertifikatsnehmer generiert. Die Generierung des Schlüsselmaterials erfolgt in diesem Fall durch Hardware. Die Hardware Crypto-Komponenten auf der Smart Card sind nach FIPS 140-2 Level 3 zertifiziert.

Im Gegensatz dazu findet die Generierung des Verschlüsselungsschlüsselpaares durch Software Crypto-komponenten statt. Dies ermöglicht eine Archivierung von Verschlüsselungsschlüsseln. Die Software Crypto-Komponenten sind nach FIPS 140-2 Level 1 zertifiziert.

6.1.2. Auslieferung der privaten Schlüssel an Zertifikatsnehmer

Private Schlüssel der Commerzbank Zertifizierungsstellen:

Jeglicher Prozess, der den Zugriff auf den privaten Schlüssel der Zertifizierungsstelle erforderlich macht, ist das HSM zwingend eingebunden; alle privaten CA Schlüssel liegen nur in der HSM selbst vor.

Eine Auslieferung des privaten Schlüsselmaterials von CA Schlüsseln ist nicht notwendig, da die HSM für die Schlüsselerzeugung und als sichere Ablage für private Schlüssel dient. Als Ablage des privaten Schlüsselmaterials auf der HSM dienen Backup Token.

Private Schlüssel für Commerzbank Benutzerzertifikate auf Smart Cards;

Die Smart Card wird an den Commerzbank Zertifikatsnehmer ausgeliefert. Im Auslieferungszustand ist die Smart Card ohne Schlüsselpaare und Zertifikate. In Rahmen der Smart Card Provisionierung werden die Schlüsselpaare für Benutzerzertifikate auf der eingesetzten Smart Card generiert, oder im Falle von Verschlüsselungsschlüssel nachträglich aufgebracht.

Der Zugriff auf den privaten Schlüssel wird erst nach erfolgreicher Freischaltung durch einen Benutzer PIN gewährt.

Private Schlüssel der Commerzbank Gruppenpostfach Zertifikate:

Die Schlüsselpaare werden selbst auf den beantragenden Maschinen generiert.

Eine nachträgliche manuelle Auslieferung ist nicht notwendig. In diesem Fall erfolgt die Auslieferung des privaten Schlüssels automatisiert an die Antragsmaschine über geeignete sichere Verfahren, wie PKCS#12.

6.1.3. Auslieferung der öffentlichen Schlüssel an Zertifikatsaussteller

Der Certificate Signing Request (CSR) des Zertifikatnehmers wird durch die Personen PKI an die Zertifizierungsstelle zum Zwecke der Zertifizierung im PKCS#10 Format übermittelt. Der gesamte Prozess findet automatisiert statt.

Der Certificate Signing Request der Commerzbank AG Inhouse Sub CA 03 erfolgt auch im PKCS#10 Format. Allerdings findet dieser Prozess, aufgrund der Offline-Mimik der Commerzbank AG Inhouse Root CA, rein manuell statt.

6.1.4. Auslieferung der öffentlichen CA Schlüsseln an vertrauende Parteien

Die Auslieferung der öffentlichen CA Schlüsseln erfolgt manuell. Des Weiteren sind die öffentlichen Schlüssel der Commerzbank Zertifizierungsstellen auf dafür vorgesehenen Web-URLs publiziert:

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

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

6.1.5. Schlüssellängen

Commerzbank CA Schlüssellänge:

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

Commerzbank Zertifikatsnehmer Schlüssellänge:

- Commerzbank Benutzerzertifikate für Smart Cards – 2048bit – RSA Algorithmus
- Commerzbank Zertifikate für Gruppenpostfächer – 2048bit – RSA Algorithmus

6.1.6. Erzeugung und Prüfung der Schlüsselparameter

- Public Key Algorithmus: 1.2.840.113549.1.1.1 (RSA)
- Signaturalgorithmus: 1.2.840.113549.1.1.5 (sha1RSA)

6.1.7. Schlüsselverwendungszweck (wie im X.509 Version 3 Key Usage Feld)

Siehe auch in Abschnitt 7.1 Zertifikats- und CRL Profile

Commerzbank CA Schlüsselverwendung:

- Commerzbank AG Inhouse Root CA – Digital Signature, Certificate Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline)
- Commerzbank AG Inhouse Sub CA 03 – Digital Signature, Certificate Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline)

Commerzbank Zertifikatsnehmer Schlüsselverwendung:

- Commerzbank Gruppenpostfächer – Key Encipherment
- Commerzbank Smart Card (Authentication) – Digital Signature
- Commerzbank Smart Card (Encryption) – Key Encipherment
- Commerzbank Smart Card (Signature) – Digital Signature, Non-Repudiation

6.2. Schutz des privaten Schlüssels und kryptographische Module

In der Commerzbank Personen PKI wird privates Schlüsselmaterial durch kryptographische Module in der Ausprägung als Hardware oder Software geschützt.

Der Schutz des privaten Schlüsselmaterials von Commerzbank Zertifizierungsstellen wird durch das Hardware Security Modul und des privaten Schlüsselmaterials von Commerzbank Zertifikatsnehmern durch eine Software und Hardware Implementierung der Crypto-Schnittstelle umgesetzt.

Der Schutz des privaten Schlüsselmaterials von:

- Commerzbank Zertifizierungsstellen wird durch das Hardware Security Modul
- Commerzbank Zertifikate für Smart Cards wird durch eine wird durch eine Hardware Implementierung der Crypto-Schnittstelle auf der Smart Card
- Commerzbank Zertifikate für Gruppenpostfächer wird durch eine Software Implementierung der Crypto-Schnittstelle

realisiert.

6.2.1. Standards und Sicherheitsmassnahmen von kryptographischen Modulen

- Das eingesetzte Netzwerk HSM ist nach FIPS 140-2, Level 2 and Level 3 evaluiert.
- Die eingesetzten Smart Cards sind nach FIPS 140-2, Level 3 evaluiert.
- Die eingesetzten Software Crypto-Module sind nach FIPS 140-2, Level 1 evaluiert.

6.2.2. Mehr-Personenkontrolle von privaten Schlüsseln (n von m Verfahren)

Eine Schlüsselteilung von privaten Schlüsseln findet nicht statt. Ausnahme bildet der Betrieb der Netzwerk HSM. Ein n-von-m Verfahren für die Netzwerk HSM Verwaltung wurde eingerichtet.

6.2.3. Hinterlegung von privaten Schlüsseln

Private Schlüssel der Commerzbank Zertifizierungsstellen werden mittels HSM Backup Token hinterlegt.

6.2.4. Backup von privaten Schlüsseln

Privates Schlüsselmaterial der Commerzbank Zertifizierungsstellen wird durch die Netzwerk HSM und zugehörigen HSM Backup Token und Prozesse gesichert.

Privates Schlüsselmaterial der Commerzbank Zertifikatsnehmer für Verschlüsselungsschlüssel wird durch das Personen PKI angebotenen Backup Mechanismen gesichert. Eine Detailbeschreibung der beiden o. g. Prozesse können bei der GS-ITR 4.3 erfragt werden.

6.2.5. Archivierung von privaten Schlüsseln

Private Schlüssel werden nur für Verschlüsselungsschlüssel hinterlegt. Zur Wiederherstellung von privatem Schlüsselmaterial steht ein Schlüssel Backup/Archiv zur Verfügung. Detailinformationen können bei der GS-ITR 4.3 erfragt werden.

6.2.6. Transfer von privaten Schlüsseln in oder aus einem kryptographischen Modul

Ein Transfer von privaten Schlüsseln ist nur für Versschlüsselungsschlüsseln vorgesehen. Hierzu wird das Schlüsselmaterial außerhalb des kryptographischen Moduls (Smart Cards) generiert und nachgelagert in das kryptographische Modul (Smart Card) importiert. Dieses Verfahren ist notwendig um Verschlüsselungsschlüsselmaterial zu archivieren.

Privates Schlüsselmaterial der Commerzbank Zertifizierungsstellen wird durch die Netzwerk HSM eigenen Backup Komponenten (Backup Token) und Prozesse gesichert.

6.2.7. Ablage von privaten Schlüsseln im kryptographischen Modul

Die privaten Schlüssel der Commerzbank AG Inhouse Root CA und der Commerzbank AG Inhouse Sub CA 03 werden durch das Netzwerk HSM verwaltet und geschützt. Darüber hinaus wird ein Backup der CA Schlüssel durch das Netzwerk HSM ausgeführt, diese wiederum sind in einer physisch geschützten Umgebung abgelegt. Das Netzwerk HSM ist nach FIPS 140-2, Level 3 zertifiziert.

Die privaten Schlüssel für Benutzerzertifikate auf Smart Cards werden durch die eingesetzte Smart Card geschützt und in einem gesicherten Bereich auf der Smart Card abgelegt. Die eingesetzten Smart Cards sind nach FIPS 140-2, Level 3 zertifiziert.

Die privaten Schlüssel für die Commerzbank Gruppenpostfächerwerden auf der beantragenden Maschine durch eine Software Crypto-Komponente verwaltet und gesichert abgelegt. Die Software Crypto-Komponenten sind nach FIPS 140-2 Level 1 zertifiziert.

6.2.8. Aktivierung der privaten Schlüssel

Eine Aktivierung von privaten Schlüsseln ist nur für Commerzbank Benutzerschlüssel auf Smart Cards vorgesehen. Die Aktivierung und damit auch der Zugriff auf den privaten Schlüssel erfolgt durch Festlegung einer Smart Card PIN durch den Benutzer.

6.2.9. Deaktivierung der privaten Schlüssel

Nicht zutreffend. Eine Deaktivierung von privaten Schlüsseln ist für die Commerzbank Personen PKI nicht vorgesehen.

6.2.10. Vernichtung der privaten Schlüssel

Die Methoden zur Vernichtung privater Schlüssel durch den Zertifizierungsdienstanbieter hängen von der kryptographischen Hardware und/oder der kryptographischen Software ab, in der die Schlüssel gespeichert werden:

- Die Vernichtung des gesamten privaten Schlüsselmaterials erfolgt in der Regel durch das Löschen des privaten Schlüsselspeichers. Eine individuelle Löschung von privaten Schlüsseln muss manuell umgesetzt werden.
- Private CA Schlüssel, die in HSMs gespeichert werden, werden durch das Löschen des Schlüssels im HSM vernichtet.
- Private Schlüssel, die auf Smart Cards vorliegen werden durch eine Initialisierung bzw. Formatierung gelöscht.

6.2.11. Bewertung des kryptographischen Moduls

- Das eingesetzte Netzwerk HSM wird nach FIPS 140-2, Level 3 betrieben.
- Die eingesetzten Smart Cards werden nach FIPS 140-2, Level 3 betrieben.
- Die eingesetzten Software Krypto-Module werden nach FIPS 140-2, Level 1 betrieben.

6.3. Weitere Aspekte für die Verwaltung von Schlüsselpaaren

6.3.1. Archivierung der öffentlichen Schlüssel

Alle von den Zertifizierungsdiensten ausgestellten Zertifikate werden in der Zertifizierungsstellen-datenbank archiviert. Darüber hinaus findet keine Archivierung öffentlicher Schlüssel statt.

6.3.2. Gültigkeit von Zertifikaten und Schlüsselpaaren.

Für die Commerzbank AG Zertifizierungsstellen sind folgende Lebensdauern festgelegt:

Commerzbank AG Inhouse Root CA

- Root CA Zertifikat: 30 Jahre
- Root CA CRLs: 4 Monate
- Zertifikatserneuerung mit Schlüsselwechsel

Commerzbank AG Inhouse Sub CA 03

- Sub CA 03 Zertifikat: 10 Jahre
- Sub CA 03 CRLs: 14 Tage
- Zertifikatserneuerung mit Schlüsselwechsel

Commerzbank AG Zertifikate für Smart Cards

- Commerzbank Smart Card Zertifikate: 3 Jahre
- Zertifikatserneuerung mit Schlüsselwechsel

Commerzbank AG Zertifikate für Gruppenpostfächer

- Commerzbank Gruppenpostfach Zertifikat: 3 Jahre
- Zertifikatserneuerung mit Schlüsselwechsel

6.4. Aktivierungsdaten

In Rahmen der Commerzbank Personen PKI Implementierung fallen Aktivierungsdaten an, welches den Zugriff auf das private Schlüsselmaterial kontrolliert.

Aktivierungsdaten werden bei der Ausgabe von Smart Cards eine Benutzer PIN und PUK, für Commerzbank Benutzer erstellt.

6.4.1. Erzeugung der Aktivierungsdaten und Installation

Die zufallsgenerierte Erzeugung der Aktivierungsdaten (PUK) erfolgt durch das Zertifikats- und Smart Card Managementsystem.

6.4.2. Schutz der Aktivierungsdaten

Aktivierungsdaten (PUK) werden durch das Zertifikats- und Smart Card Managementsystem geschützt. Hierzu werden diese Daten verschlüsselt auf der zugehörigen Zertifikatsmanagementdatenbank abgelegt. Der Zugriff auf diese erfolgt exklusiv nur für das Managementsystem.

6.4.3. Weitere Aspekte von Aktivierungsdaten

Nicht zutreffend.

6.5. Sicherheitsmaßnahmen für Computer

6.5.1. Spezifische technische Anforderungen von Sicherheitsmaßnahmen für Computer

Für Server, die zentrale Funktionen der Zertifizierungsdienste implementieren, sowie alle Rechner, die dem Schutz der Einrichtungen der Zertifizierungsdienste dienen, gelten die folgenden Sicherheitsanforderungen:

- Auf dem Server ist nur die für die jeweilige Funktion notwendige Software installiert.
- Der Server besitzt nur die für die jeweilige Funktion notwendigen Kommunikationsschnittstellen. Insbesondere sind die Rechner nur in die für ihre Funktion notwendigen Teilnetzwerke integriert.
- Unnötige Funktionen des Betriebssystems und der installierten Software werden – sofern möglich – deaktiviert.
- Falls Sicherheitsrisiken in der verwendeten Software bekannt werden, ergreifen die Systemadministratoren zeitnah die vom Hersteller bzw. von unabhängigen Experten empfohlenen Gegenmaßnahmen. Insbesondere werden beim Betriebssystem und der Software stets die aktuellen Patches gegen bekannte Sicherheitslücken eingespielt.
- Der Zugriff auf die Server ist auf das für den Betrieb der Zertifizierungsdienste notwendige Maß beschränkt. Insbesondere werden die Server nur durch die verantwortlichen Systemadministratoren verwaltet.
- Sicherheitskritische Ereignisse auf den Rechnern werden protokolliert.
- Systeme mit hohen Verfügbarkeitsanforderungen sind hochverfügbar ausgelegt, so dass bei Ausfall eines Rechners die Funktion erhalten bleibt.

- Mittels unterbrechungsfreier Stromversorgungen und mittels Aggregaten werden Schwankungen in der Stromversorgung ausgeglichen und Stromausfälle bis zu einer Dauer von mehreren Stunden überbrückt.
- Auf den Systemen dürfen nur nach Viren geprüfte Datenträger verwendet werden.

6.5.2. Bewertung der Computersicherheit

Die Commerzbank Personen PKI baut auf Zertifizierungsdiensten auf, die nach Common Criteria EAL (Evaluation Assurance Level) 4+ (FLR – augmented with Flow Remediation) evaluiert sind.

Das eingesetzte Netzwerk HSM ist nach FIPS 140-2, Level 2 and Level 3 evaluiert.

Die eingesetzten Smart Cards sind nach FIPS 140-2, Level 3 evaluiert.

Die eingesetzten Software Krypto-Module sind nach FIPS 140-2, Level 1 evaluiert.

6.6. Technische Kontrollen für den gesamten Lebenszyklus

6.6.1. Sicherheitsmassnahmen bei der Systementwicklung

Nicht zutreffend.

6.6.2. Sicherheitsmanagement

Nicht zutreffend.

6.6.3. Sicherheitsmaßnahmen für den gesamten Lebenszyklus

In Rahmen des Sicherheitskonzeptes für das Commerzbank Personen PKI und die zugehörigen Zertifizierungsstellen werden die notwendigen Sicherheitsmaßnahmen beleuchtet.
Detailinformation zum Sicherheitskonzept können bei Bedarf von der GS-ITR 4.3 erfragt werden.

6.7. Sicherheitsmaßnahmen im Netz

Die Zertifizierungsdienste implementieren die folgenden Maßnahmen zur Netzwerksicherheit:

- Die produktiven Systeme und Netzwerke sind durch Firewalls vom Internet getrennt.
- Die internen Netzwerke der Zertifizierungsdienste sind soweit möglich nach dem Schutzbedarf der Systeme aufgeteilt. Die Trennung in Teilnetze erfolgt durch Firewalls.
- Firewalls beschränken den Datenverkehr auf das für den Betrieb notwendige Maß.

6.8. Zeitstempel

Die Commerzbank Zertifizierungsstellen nutzen Zeitstempel bei der Ausgabe von Zertifikaten und Zertifikatssperrlisten. Die verwendete Zeitquelle ist hierbei die lokale Systemuhr des verwendeten Computersystems. Die lokale Systemuhr der Online Server wird regelmäßig mit einer externen Zeitquelle automatisch synchronisiert. Die Zeitsynchronisation der Commerzbank Inhouse Root CA erfolgt manuell.

Der Einsatz einer vertrauenswürdigen und evaluierten Zeitstempelkomponente ist für die Personen PKI Lösung nicht notwendig.

7. Zertifikats- und CRL Profil

In Rahmen der Personen PKI sind Zertifikats- und CRL Profile für die Commerzbank AG Inhouse Root CA definiert. Diese Profile folgen den PKIX Vorgaben nach RFC 5280 und haben insbesondere die Interoperabilitätsaspekte im Fokus. Erweiterungen für die Zertifikats- und CRL Profile sind vorgesehen, soweit diese zum Zwecke der Unterscheidung von Zertifikatstypen genutzt werden können.

7.1. Zertifikatsprofil

Commerzbank Zertifikate entsprechen:

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

Commerzbank Zertifikatsprofile sind konform:

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

Die Basisbeschreibung von Commerzbank Zertifikaten enthält:

Feld	**Wert**
Version	Siehe auch *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. Siehe auch *7.1.3. Algorithm Object Identifiers*
Issuer	siehe auch *7.1.4. Name Forms*
Validity	Validity (from and to) time and date information.'
Subject	siehe auch *7.1.4. Name Forms*
Subject Public Key	Public Key Blob
Signature	CAs signature

Commerzbank AG CA Zertifikate

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

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

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

Authority Information Access	http://ca.commerzbank.com/aia/coba_root.crt
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	sha1
Thumbprint	11 cd e7 32 6d a3 5e e1 42 fc 99 4f 70 af ad fd c4 c4 6e 66

Commerzbank AG Smart Card Zertifikate

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

Coba SC Signature	
X.509 Version	V3

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

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

	L = Frankfurt am Main C = DE
Key Usage	Key Encipherment
Subject Key Identifier	[corresponding private key]
Authority Key Identifier	d5 b6 fa fa 21 9f 06 eb c4 f2 cb f7 36 60 cb 3b 8c f0 3f a0
CRL Distribution Points	http://ca.commerzbank.com/cdp/coba_sub03.crl
Authority Information Access	http://ca.commerzbank.com/aia/coba_sub03.crt
Subject Alternative Name	<RFC 822 eMail address>
Extended Key Usage	BitLocker-Laufwerkverschlüsselung (1.3.6.1.4.1.311.67.1.1) Sichere E-Mail (1.3.6.1.5.5.7.3.4) Verschlüsselndes Dateisystem (1.3.6.1.4.1.311.10.3.4)
Thumbprint Algorithm	sha1
Thumbprint	[Thumbprint of certificate]

Commerzbank AG Zertifikate für Gruppenpostfächer

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

Extended Key Usage	Sichere E-Mail (1.3.6.1.5.5.7.3.4)
Thumbprint Algorithm	sha1
Thumbprint	[Thumbprint of certificate]

7.1.1. Version Number(s)

Die Commerzbank AG Inhouse Root CA und die Commerzbank AG Inhouse Sub CA 03 stellen X.509 Version 3 Zertifikate aus.

7.1.2. Certificate Extensions

Folgende Zertifikatserweiterungen werden in den von der Commerzbank bereitgestellten Zertifikaten berücksichtigt:

Erweiterung	Wert	Kritisch
Key Usage	Digital Signature, Certificate Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline), Key Encipherment, Non Repudiation	Nein
Subject Key Identifier	Unique number corresponding to the subject's public key. The key identifier method is used.	Nein
Authority Key Identifier	Unique number corresponding to the authority's public key. The key identifier method is used.	Nein
CRL Distribution Point	Contains the information where the current CRL can be obtained	Nein
Authority Information Access	Contains a link where additional information to the issuing CA can be obtained (ca issuers method)	Nein
Extended Key Usage	Contains application specific attributes/OIDs	Nein
Subject Alternative Name	Contains alternative Subject Names, such as eMail address or UPN	Nein
Certificate Issuance Policies	1.3.6.1.4.1.14978.5.1 (Commerzbank AG CP/CPS OID Referenz)	Nein

Folgende private Zertifikatserweiterungen kommen zur Anwendung:

Erweiterung	OID	Kritisch
Certificate Template Information	1.3.6.1.4.1.311.21.7	Nein
Application Policies	1.3.6.1.4.1.311.21.10	Nein

7.1.3. Algorithm Object Identifiers

- Die Commerzbank Zertifizierungsstellen erstellen RSA Schlüsselpaare (OID: 1.2.840.113549.1.1.1) gemäß RFC 5280.

- Die Commerzbank Zertifizierungsstellen erstellen Signaturen mit sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) gemäß RFC 5280.

7.1.4. Name Forms

Die von der **Commerzbank AG Inhouse Root CA** ausgestellten **CA Zertifikate** enthalten den kompletten DN (Distinguished Name) im Subject Name und im Issuer Name Feld. Der Aufbau des DNs erfolgt gemäß X.500 und enthält die Komponenten in folgender Reihenfolge:

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

Die von der **Commerzbank AG Inhouse Sub CA 03** ausgestellten **End-Entitäten Zertifikate** enthalten den kompletten DN (Distinguished Name) im Subject Name und im Issuer Name Feld. Der Aufbau des DNs erfolgt gemäß X.500 und enthält die Komponenten in folgender Reihenfolge:

Für Zertifikatstyp **CoBa SC Authentication** gilt:
CN = [Common Name],
O = [Organization],
L = [Locality],
C = [Country]

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

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

7.1.5. Name Constraints

nicht zutreffend. Es existieren keine Beschränkungen bezogen auf Namen.

7.1.6. Certificate Policy Object Identifier

Die Commerzbank AG Certificate Policy OID für die Root CA lautet: 1.3.6.1.4.1.14978.5.1

7.1.7. Policy Constraints Extension

nicht zutreffend.

7.1.8. Policy Qualifiers Syntax und Semantik

Die Commerzbank Certificate Policy Qualifier ID ist: CPS.

- Commerzbank PKI OID:
- 1.3.6.1.4.1.14978.5.1

Die Commerzbank CPS Lokation wird durch eine URL bereitgestellt:

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

7.1.9. Processing Semantics für kritische Certificate Policies Extension

nicht zutreffend

7.2. CRL Profil

CRLs werden in Rahmen der Commerzbank Personen PKI ausgegeben. Eine Ausgabe von deltaCRLs ist im Falle der Commerzbank Root CA nicht geplant.

Commerzbank CRL Profile entsprechen:

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

Commerzbank CRL Profile sind konform:

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

Die Basis CRL Felder sind wie folgt festgelegt:

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

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

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

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

7.2.1. Version Number(s)

Die Commerzbank Root CA stellt CRLs auf Basis X.509 Version 2 aus.

7.2.2. CRL und CRL Entry Extensions

CRL Extensions (Erweiterungen) können aus dem aktuell für die Commerzbank Root CA geltenden CRL Profil entnommen werden. Siehe auch *7.2. CRL Profile*.

7.3. OCSP Profil

nicht zutreffend. OCSP wird durch die Commerzbank Personen PKI nicht unterstützt.

7.3.1. Version Number(s)

nicht zutreffend.

7.3.2. OCSP Extensions

nicht zutreffend.

8. Auditierung und Überprüfung der Konformität

In Rahmen der Commerzbank Personen PKI werden interne Audits durchgeführt, um Abweichungen vom Regelbetrieb der Commerzbank PKI zu den Ausführungen in der Commerzbank Certificate Policy bzw. Certification Practice Statement (CP/CPS) zu identifizieren, und bei aufgedeckten Abweichungen der Konformität notwendige korrektive Maßnahmen zu ergreifen.

8.1. Frequenz und Umstand der Überprüfung

Grundsätzlich sind interne Audits und Überprüfungen in regelmäßigen Abständen geplant. Frequenz und Umstände, die zu einer Überprüfung führen können, werden durch die Commerzbank Revision festgelegt.

8.2. Identität und Qualifikation des Prüfers/Auditors

Es wird vorgesehen, dass nur interne Commerzbank AG Mitarbeiter die Konformitätsüberprüfung durchführen. Das Auditierungspersonal sollte über Know-how aus der Auditierung im Sicherheitsumfeld besitzen, insbesondere die notwendigen Kenntnisse aus dem Bereich der Public Key Infrastructure (PKI) und aus dem Bereich des Rechenzentrumsbetriebes (ITIL-Zertifizierung) sind erforderlich.

8.3. Verhältnis des Prüfers zur überprüften Entität

Der zugewiesen Auditor für die Überprüfung der Konformität ist zur überprüften Entität, nämlich der Commerzbank AG Personen PKI (Technologie und Prozesse) organisatorisch unabhängig.

8.4. von der Überprüfung abgedeckte Bereiche

Die von einer Überprüfung betroffenen Bereiche werden jeweils durch die Commerzbank Revision festgelegt. Für Umstände, die zwingend eine Überprüfung notwendig machen, können bestimmte Bereiche von vornherein festgelegt werden.

Dazu gehören unter anderem:

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

8.5. Maßnahmen bei Nichterfüllung oder Abweichen von der Konformität

Werden Abweichungen zur Konformität festgestellt so müssen diese zeitnah korrigiert werden. Hierzu wird ein Aktionsplan entwickelt, welche die notwendigen Maßnahmen beschreiben um die notwendigen Korrekturen auszuführen.

Nach Umsetzung des Aktionsplans gilt es zu überprüfen ob die ausgeführten Maßnahmen zu einer Korrektur der Mängel geführt haben. Die Commerzbank IT Management und die Commerzbank Revision wird über die erzielten Ergebnisse informiert.

8.6. Kommunikation der Prüfergebnisse

Die Ergebnisse der Auditierung bzw. Prüfung werden als vertraulich erachtet und sind nicht bestimmt für die Öffentlichkeit.

9. Weitere rechtliche und geschäftliche Regelungen

Dieser Abschnitt bezieht sich auf die geschäftlichen-, rechtlichen- und Datenschutz-Aspekte der Commerzbank Personen PKI.

9.1. Gebühren

Die Gebühren für Dienstleistungen, die durch die von der Commerzbank AG betriebenen Zertifizierungsstellen erbracht werden, sind der internen Verrechnungstabelle zu entnehmen. Diese kann bei der in Abschnitt 1.5.2 angegebenen Kontaktperson abgerufen werden.

9.1.1. Gebühren für die Ausstellung und Erneuerung von Zertifikaten

Detailinformation ist der internen Verrechnungstabelle der Commerzbank für den Personen PKI Dienst zu entnehmen.

9.1.2. Gebühren für den Zugriff auf Zertifikate

Detailinformation ist der internen Verrechnungstabelle der Commerzbank für den Personen PKI Dienst zu entnehmen.

9.1.3. Gebühren für den Zugriff auf Speerlisten- oder Status-Information

Detailinformation ist der internen Verrechnungstabelle der Commerzbank für den Personen PKI Dienst zu entnehmen.

9.1.4. Gebühren für weitere Dienste

Detailinformation ist der internen Verrechnungstabelle der Commerzbank für den Personen PKI Dienst zu entnehmen.

9.1.5. Richtlinie für die Erstattung von Gebühren

Detailinformation ist der internen Verrechnungstabelle der Commerzbank für den Personen PKI Dienst zu entnehmen.

9.2. Finanzielle Verantwortung

9.2.1. Versicherungsschutz

Ein Versicherungsschutz ist nicht gegeben.

9.2.2. Vermögenswerte

Vermögenswerte werden nicht abgedeckt.

9.2.3. Versicherungsschutz oder Gewährleistung für Zertifikatsnehmer

Ein Versicherungsschutz für Zertifikatnehmer ist nicht gegeben.

9.3. Vertraulichkeit von Geschäftsinformationen

9.3.1. Vertrauliche Informationen berücksichtigt

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter 9.3.2 fallen, werden als vertrauliche Informationen eingestuft. Zu diesen Informationen zählen u. a. Geschäftspläne, Vertriebsinformationen, Informationen über Geschäftspartner und ebenso alle Informationen, die beim Registrierungsprozess zur Kenntnis gekommen sind.

9.3.2. Vertrauliche Informationen nicht berücksichtigt

Jegliche Informationen, die in den herausgegebenen Zertifikaten und Widerrufslisten explizit (z.B. e-Mail Adresse) oder implizit (z.B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

9.3.3. Verantwortung zum Schutz vertraulicher Informationen

Jede innerhalb der Commerzbank Personen PKI operierende Zertifizierungsstelle trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

9.4. Datenschutz (personenbezogen)

9.4.1. Datenschutzrichtlinie/-plan

Die Speicherung und Verarbeitung von personenbezogenen Daten richtet sich nach den gesetzlichen Datenschutzbestimmungen.

9.4.2. Vertraulich zu behandelnde Informationen

Jegliche Informationen über Zertifikatsnehmer und Antragsteller sind vertraulich zu behandeln.

9.4.3. Nicht vertraulich zu behandelnde Informationen

Nicht vertraulich sind Informationen die in den öffentlichen Zertifikaten, wie im Commerzbank Zertifikat oder im Zertifizierungsstellen-Zertifikat, enthalten sind. Ebenfalls gilt es für Informationen, die in den öffentlichen Zertifikatssperrlisten (CRLs) enthalten sind.

9.4.4. Verantwortung zum Schutz personenbezogener Information

Der Commerzbank PKI Betrieb ist verantwortlich für den Schutz vertraulicher Informationen. Eine Offenlegung von vertraulichen Informationen kann nur in Abstimmung mit den verantwortlichen Stellen geschehen. Näheres hierzu kann bei der GS-ITR 4.3 erfragt werden.

9.4.5. Benachrichtigung bei Nutzung personenbezogener Information

Der Zertifikatnehmer stimmt der Nutzung von personenbezogenen Daten durch eine Zertifizierungsstelle zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden.

9.4.6. Offenlegung bei gerichtlicher Anordnung oder in Rahmen einer gerichtlichen Beweisführung

Die Commerzbank AG richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten den gesetzlichen Datenschutzbestimmungen. Eine Offenlegung findet nur gegenüber staatlichen Instanzen statt, wenn entsprechende Anordnungen ausgegeben wurden.

9.4.7. Andere Umstände einer Veröffentlichung

Keine.

9.5. Urheberrechte

Die Commerzbank AG besitzt die Urheberrechte für ausgegebene Dokumentationen in Rahmen der Personen PKI.

9.6. Verpflichtungen

9.6.1. Verpflichtung der Zertifizierungsstellen

Die Commerzbank AG Zertifizierungsstellen verpflichten sich den aufgestellten Bestimmungen der CP bzw. CPS Dokumentation zu folgen.

9.6.2. Verpflichtung der Registrierungsstellen

Die Commerzbank AG Registrierungsstellen verpflichten sich den aufgestellten Bestimmungen der CP bzw. CPS Dokumentation zu folgen.

9.6.3. Verpflichtung des Zertifikatsnehmers

Die Nutzung der Zertifikate durch den Zertifikatsnehmer hat den „Commerzbank Richtlinien für den Gebrauch von Zertifikaten“ zu folgen. In Kapitel 1.4. Anwendungsbereich von Zertifikaten sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt. Außerdem muss der Zertifikatsnehmer bei der Nutzung der privaten Schlüssel seine in der Zertifikatsrichtlinie definierten Pflichten erfüllen.

9.6.4. Verpflichtung der vertrauenden Partei

Die Nutzung der Zertifikate durch vertrauende Parteien hat den zugewiesenen Zertifikatsrichtlinien seiner Organisation zu folgen. Dort sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt.

9.6.5. Verpflichtung anderer Teilnehmer

Nicht zutreffend, da keine anderen Teilnehmer vorgesehen sind.

9.7. Gewährleistung

Grundsätzlich wird keine Gewährleistung übernommen. Die Commerzbank AG stellt die notwendigen IT Ressourcen für den Betrieb der PKI zur Verfügung, aber ohne eine garantierte Verfügbarkeit.

9.8. Haftungsbeschränkung

Die Commerzbank AG übernimmt keinerlei Haftung für Sach- und Vermögensschäden. Insbesondere bei einer unsachgemäßen oder einer grob fahrlässigen Nutzung der Commerzbank Personen PKI erlischt jegliche Haftung gegenüber Dritten.

9.9. Haftungsfreistellung

Bei der unsachgemäßen Verwendung des Zertifikats und dem zu Grunde liegenden privaten Schlüssels oder einer Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung, ist die Commerzbank AG von der Haftung freigestellt.

9.10. Inkrafttreten und Aufhebung

9.10.1. Inkrafttreten

Nach Veröffentlichung der aktuellen Commerzbank CP/CPS Dokumentation tritt dies auch in Kraft. Die Veröffentlichung erfolgt auf der im Zertifikat vorgegebenen URL:

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

9.10.2. Aufhebung

Dieses Dokument ist solange gültig, bis

- es durch eine neue Version ersetzt wird oder
- der Betrieb der Commerzbank AG Zertifizierungsstellen eingestellt wird.

9.10.3. Konsequenzen der Aufhebung

Keine.

9.11. Individuelle Benachrichtigung und Kommunikation mit Teilenehmern

Die individuelle Benachrichtigung der Commerzbank Personen PKI Teilnehmer erfolgt durch die Verteilung und Zustimmung der „Commerzbank Richtlinien für den Gebrauch von Zertifikaten“.

9.12. Ergänzungen der Richtlinie

Die Ergänzung und Modifikation der CP bzw. CPS Dokumentation Teilnehmer obliegt der GS-ITR 4.3. In Abschnitt 1.5. sind entsprechende Kontaktdaten veröffentlicht.

9.12.1. Prozess für die Ergänzung der Richtlinie

Nicht zutreffend.

9.12.2. Benachrichtigungsmethode und -zeitraum

Nicht zutreffend.

9.12.3. Bedingungen für die Änderung einer OID

Nicht zutreffend.

9.13. Schiedsverfahren

Nicht zutreffend.

9.14. Gerichtsstand

Der Betrieb der Commerzbank Personen PKI unterliegt den Gesetzen der Bundesrepublik Deutschland. Der Gerichtsstand ist Frankfurt am Main, Bundesrepublik Deutschland. Dieser Gerichtsstand gilt auch für Parteien deren Wohnsitz oder der gewöhnlicher Aufenthaltsort ins Ausland verlegt wird oder unbekannt ist.

9.15. Konformität zum geltenden Recht

Die von der Commerzbank Personen PKI ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten. Die Vorgaben und Richtlinien nach Signaturgesetzt [SigG] sind daher nicht bindend für den Betrieb der Commerzbank Personen PKI.

9.16. Weitere Regelungen

9.16.1. Vollständigkeit

Alle in der CP & CPS für das Personen PKI beschriebenen Regelungen gelten zwischen den von der Commerzbank AG betriebenen Zertifizierungsstellen und deren Zertifikatnehmern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2. Übertragung der Rechte

Eine Übertragung der Rechte ist nicht vorgesehen.

9.16.3. Salvatorische Klausel

Sollten einzelne Bestimmungen dieses CP & CPS Regelwerkes unwirksam sein oder dieses Regelwerk Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.

Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung entspricht. Im Falle von Lücken, gilt dasjenige als vereinbart, was nach Sinn und Zweck dieses Vertrages vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vorn herein bedacht.

Es wird ausdrücklich vereinbart, dass sämtliche Bestimmungen dieser CP & CPS, die eine Haftungsbeschränkung, den Ausschluss oder die Beschränkung von Gewährleistungen oder sonstigen Verpflichtungen oder den Ausschluss von Schadensersatz vorsehen, als eigenständige Regelungen und unabhängig von anderen Bestimmungen bestehen und als solche durchzusetzen sind.

9.16.4. Erzwingungsklausel

Rechtliche Auseinandersetzungen, die aus dem Betrieb einer von der Commerzbank AG betriebenen Zertifizierungsstelle herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland.

Erfüllungsort und ausschließlicher Gerichtsstand ist Frankfurt am Main, Bundesrepublik Deutschland.

9.16.5. Höhere Gewalt

Die Commerzbank AG übernimmt keine Haftung für die Verletzung einer Pflicht sowie für Verzug oder Nichterfüllung im Rahmen dieses CPS, sofern dies aus Ereignissen außerhalb ihrer Kontrolle, wie z.B. höhere Gewalt, Kriegshandlungen, Epidemien, Netzausfälle, Brände, Erdbeben und andere Katastrophen, resultiert.

9.17. Andere Regelung

Keine