DEUTSCHE BUNDESBANK
EUROSYSTEM

# Certification Practice Statement

# Email-Security Certificates

# - Counterparties -

Version 1.0

# 1 Einleitung

## 1.1 Überblick

Dieses Dokument fasst die für die Benutzer und die Deutsche Bundesbank als PKI-Betreiber (Public Key Infrastructure) verbindlichen Inhalte des Sicherheits- und Zertifizierungskonzepts der Deutschen Bundesbank für den Produktivbetrieb der CA for Email-Security Counterparties in Form eines Certification Practice Statements (CPS) zusammen.

Die Gliederung erfolgt nach dem Muster des Standards RFC 3647.

Die Deutsche Bundesbank ist Mitglied der European Bridge CA (EBCA). Die von der PKI der Deutschen Bundesbank ausgestellten Zertifikate erfüllen die Voraussetzungen der fortgeschrittenen Signatur nach dem Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG).

## 1.2 Name und Kennzeichnung des Dokuments

| | |
|---|---|
| Name: | Certification Practice Statement<br>Email-Security Certificates - Counterparties - |
| Version: | 1.0 |
| Datum: | 15.06.2016 |
| OID: | 1.3.6.1.4.1.2025.590.2.11 |

## 1.3 PKI-Teilnehmer

### 1.3.1 Zertifizierungsstellen

Für die PKI der Deutschen Bundesbank (BBk-PKI) wird eine zweistufige Zertifizierungsstruktur mit einem selbstsignierten Root-Zertifikat verwendet.

Die Root-CA zertifiziert ausschließlich nachgelagerte fachliche CA's. Die der Root-CA nachgeordnete CA for Email-Security Counterparties wird verwendet, um Benutzerzertifikate für die Verschlüsselung sowie zur Signatur von Emails von Geschäftspartnern zu erstellen.

### 1.3.2 Registrierungsstellen

Den Registrierungsstellen obliegt die Überprüfung der Identität und Authentizität von Zertifikatsnehmern. Das Registrierungsverfahren ist in Ziffer 3.2.3 dargestellt.

### 1.3.3 Zertifikatsnehmer

Zertifikatsnehmer sind

- Geschäftspartner der Deutschen Bundesbank sowie
- Geschäftspartner der Bundesanstalt für Finanzmarktstabilisierung (FMSA).

Zertifikatsnehmer können dabei Personen mit einer persönlichen Email-Adresse sowie Verantwortliche (Mailstellenverantwortliche) oder Mitbenutzer (Mailstellenberechtigte) einer funktionalen Mailstelle (unpersönliche Email-Adresse) sein.

### 1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind Kommunikationspartner (Personen, Organisationen bzw. Systeme), die am zertifikatsbasierten Verfahren zur sicheren Email-Kommunikation mit der Deutschen Bundesbank bzw. der FMSA teilnehmen.

### 1.3.5 Weitere Teilnehmer

Weitere Teilnehmer können von der BBk-PKI beauftragte Dienstleister (z. B. Betreiber von Verzeichnisdiensten) sein.

## 1.4 Verwendung von Zertifikaten

### 1.4.1 Erlaubte Verwendungen von Zertifikaten

Siehe CP Email-Security Certificates - Counterparties -.

### 1.4.2 Verbotene Verwendungen von Zertifikaten

Siehe CP Email-Security Certificates - Counterparties -.

## 1.5 Verwaltung der Zertifizierungsrichtlinien

### 1.5.1 Zuständigkeit für das Dokument

Dieses CPS wird vom Betreiber der BBk-PKI gepflegt.

### 1.5.2 Ansprechpartner und Kontakt

Deutsche Bundesbank
PKI Services
Berliner Allee 14 Postfach 10 11 48
40212 Düsseldorf 40002 Düsseldorf

Telefon +49 211 874 3815/3257/2351
Telefax +49 69 709094 9922
e-Mail: pki@bundesbank.de

### 1.5.3 Prüfung der Zertifizierungsrichtlinie

Dieses CPS wird durch den Systemeigner der BBk-PKI überprüft.

Der Systemeigner der BBk-PKI stellt die Übereinstimmung des CPS mit den Vorgaben der CP Email-Security Certificates - Counterparties - sicher.

### 1.5.4 Veröffentlichung der Richtlinie

Dieses CPS wird im Intranet und auf der Homepage der Deutschen Bundesbank veröffentlicht.

Eine Weitergabe an andere Organisationen ist vorgesehen, damit eine unabhängige Überprüfung der Arbeitsweise der CA for Email-Security Counterparties der BBk-PKI möglich ist.

## 1.6 Definitionen und Abkürzungen

siehe Kapitel 10.

# 2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

## 2.1 Verzeichnisse

Die Deutsche Bundesbank stellt die Informationen zur BBk-PKI auf der Homepage

- http://www.bundesbank.de unter Service ► Service für Banken und Unternehmen ► PKI
- bzw. direkt unter http://www.bundesbank.de/Navigation/DE/Service/Services_Banken_und_Unternehmen/PKI/pki.html

sowie im Intranet (Zugriff nur für Beschäftigte der Deutschen Bundesbank, der FMSA sowie deren externe Mitarbeiterinnen und Mitarbeiter) zur Verfügung.

## 2.2 Veröffentlichung von Informationen zu Zertifikaten

Die Deutsche Bundesbank veröffentlicht die folgenden Informationen:

- CA-Zertifikate mit Fingerprints,
- Root-CA-Zertifikate mit Fingerprints,
- Sperrlisten,
- Erläuterungen zum Sperrverfahren,
- CP und CPS.

## 2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Für die Veröffentlichung von CA-/Root-CA-Zertifikaten, Sperrlisten sowie CP und CPS gelten die folgenden Intervalle:

| | |
|---|---|
| – CA-/Root-CA-Zertifikate mit Fingerprints | unmittelbar nach Erzeugung |
| – Sperrlisten | nach Sperrungen, sonst turnusmäßig (siehe Ziffer 4.9.7) |
| – CP und CPS | nach Erstellung bzw. Aktualisierung. |

## 2.4 Zugang zu den Informationsdiensten

Der lesende Zugriff auf die unter den Ziffern 2.1 und 2.2 aufgeführten Informationen ist nicht eingeschränkt. Der schreibende Zugriff liegt im Verantwortungsbereich der BBk-PKI.

# 3 Identifizierung und Authentifizierung

## 3.1 Namen

### 3.1.1 Namensform

Der Name der ausgestellten Zertifikate (Distinguished Name = DN) richtet sich nach den Vorgaben des Standards x.509.

Der DN entspricht grundsätzlich folgendem Schema:

| | |
|---|---|
| **EMAIL** | <E-Mailadresse> |
| **CN** | <Vorname Name> |
| **OU** | <Organisationseinheit> |
| **O** | <Organisation> |
| **C** | de |

### 3.1.2 Aussagekraft von Namen

Der Name des ausgestellten Zertifikates (DN) muss den Zertifikatsnehmer eindeutig identifizieren. Es gelten die folgenden Regelungen:

- Zertifikate für natürliche Personen sind auf den Namen des Zertifikatsnehmers auszustellen.
- Zertifikate für organisations- bzw. funktionsbezogene Personengruppen sowie für organisationsbezogene Mailstellen müssen sich deutlich von Zertifikaten für natürliche Personen unterscheiden.

### 3.1.3 Anonymität oder Pseudonymität von Zertifikatsinhabern

Siehe CP Email-Security Certificates - Counterparties -.

### 3.1.4 Regeln zur Interpretation verschiedener Namensformen

Der DN richtet sich nach den Vorgaben des Standards x.509.

### 3.1.5 Eindeutigkeit von Namen

Siehe CP Email-Security Certificates - Counterparties -.

### 3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Siehe CP Email-Security Certificates - Counterparties -.

## 3.2 Identitätsüberprüfung bei Neuantrag

### 3.2.1 Nachweis des Besitzes des privaten Schlüssels

Siehe CP Email-Security Certificates - Counterparties -.

### 3.2.2 Authentifizierung einer Organisation

Zertifikate für organisationsbezogene Mailstellen bzw. organisations- oder funktionsbezogene Personengruppen werden immer von natürlichen Personen beantragt, deren Authentifizierung gemäß Ziffer 3.2.3 erfolgt.

### 3.2.3 Authentifizierung natürlicher Personen

Beschäftigte berechtigter Geschäftspartner der Deutschen Bundesbank sowie der FMSA werden im Rahmen der Zertifikatsbeantragung über eine Kopie eines amtlichen Lichtbildausweises authentifiziert, die an die BBk-PKI weitergeleitet wird. Die Ausweiskopie wird von der BBk-PKI nach Auslieferung des Zertifikates vernichtet.

### 3.2.4 Nicht überprüfte Zertifikatsnehmer Informationen

Es werden nur Angaben zur Authentifikation und Identifikation von Zertifikatsnehmern überprüft. Andere Informationen des Zertifikatsnehmers werden nicht berücksichtigt.

### 3.2.5 Prüfung der Berechtigung zur Antragstellung

Die Beantragung von Zertifikaten erfolgt im Rahmen eines mehrstufigen elektronischen Antragsworkflows, der von der jeweiligen Fachstelle zu genehmigen ist.

### 3.2.6 Kriterien für Cross-Zertifizierung und Interoperabilität

Siehe CP Email-Security Certificates - Counterparties -.

## 3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

### 3.3.1 Routinemäßige Zertifikatserneuerung

Die Zertifikatsnehmer werden von der BBk-PKI über den Ablauf der Gültigkeit des Zertifikates unterrichtet.

Eine Zertifikatserneuerung sowie die damit einhergehende Identifizierung und Authentifizierung erfolgt analog zum initialen Antragsprozess auf Initiative von Beschäftigen der Deutschen Bundesbank bzw. der FMSA.

### 3.3.2 Zertifikatserneuerung nach einer Sperrung

Nach der Sperrung eines Zertifikates muss ein Neuantrag gestellt werden.

## 3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperrung eines Zertifikates kann vom Zertifikatsnehmer, einem vom Zertifikatsnehmer Beauftragten oder vom Vorgesetzten telefonisch als auch per Telefax oder schriftlich veranlasst werden.

Die Identität des Antragstellers wird hierbei dokumentiert. Die Betriebsstelle der BBk-PKI behält sich vor, die Identität des Antragstellers zu überprüfen, sie ist jedoch nicht dazu verpflichtet. Der Zertifikatsnehmer wird über die Sperrung des Zertifikates unterrichtet.

# 4 Ablauforganisation

## 4.1 Zertifikatsantrag

### 4.1.1 Wer kann ein Zertifikat beantragen

Die Beantragung eines Zertifikates für einen Geschäftspartner erfogt auf Initiative von Beschäftigten der Deutschen Bundesbank bzw. der FMSA über einen elektronischen Antragsworkflow, der nach Genehmigung durch den direkten Vorgesetzten des Beschäftigten der Deutschen Bundesbank bzw. der FMSA an die BBK-PKI übersendet wird.

Ein im Rahmen des elektronischen Antragsprozesses zu erzeugendes Antragsformular wird dem Geschäftspartner von der BBk-PKI zur Unterschrift übersandt.

### 4.1.2 Registrierungsprozess und Zuständigkeit

Die Beantragung von Zertifikaten erfolgt im Rahmen eines mehrstufigen elektronischen Antragsworkflows über die genehmigende Dienststelle an die BBk-PKI.

Bei der Beantragung erkennt der Antragssteller ausdrücklich die Gültigkeit des CPS der austellenden CA an.

Siehe auch CP Email-Security Certificates - Counterparties -.

## 4.2 Bearbeitung von Zertifikatsanträgen

### 4.2.1 Durchführung der Identifikation und Authentifizierung

Die Identifikation und Authentifizierung von Zertifikatsnehmern wird gemäß Kapitel 3.2 durchgeführt.

### 4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Siehe CP Email-Security Certificates - Counterparties -.

### 4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

Siehe CP Email-Security Certificates - Counterparties -.

## 4.3 Ausstellung von Zertifikaten

### 4.3.1 Aufgaben der Zertifizierungsstelle

Nach der Bearbeitung des Zertifikatsantrages wird das Schlüsselpaar im Sicherheitsbereich der BBk-PKI im Vier-Augen-Prinzip erstellt und das Zertifikat erzeugt.

Die Beauftragung eines Zertifikats erfolgt über einen elektronischen Antragsworksflow sowie ein Antragsformular des Zertifikatsnehmers. Die Zertifikatsdaten werden manuell über gesicherte Token in die offline betriebene BBk-PKI übertragen. Der nachfolgende Zertifizierungsprozess erfolgt automatisiert, wird jedoch manuell gestartet.

Die Auslieferung an den Antragsteller erfolgt nur als Software-Zertifikat. Das Zertifikat wird dabei durch eine Transport-PIN geschützt. Die Zustellung des Zertifikates erfolgt mittels gesicherter elektronischer Verfahren gegen Empfangsbestätigung. Die Transport-PIN wird dem Antragsteller in einem zweiten Schritt mittels gesicherter elektronischer Verfahren gegen Empfangsbestätigung bzw. telefonisch übermittelt.

#### 4.3.2 Benachrichtigung des Zertifikatsnehmers

Siehe CP Email-Security Certificates - Counterparties -.

## 4.4 Zertifikatsakzeptanz

Siehe CP Email-Security Certificates - Counterparties -.

## 4.5 Verwendung des Schlüsselpaars und des Zertifikats

Siehe CP Email-Security Certificates - Counterparties -.

## 4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Certificate Renewal)

Eine Zertifikatserneuerung auf Basis des bestehenden Schlüsselpaares ist nicht zugelassen. Bei der Zertifikatserneuerung wird immer ein neues Schlüsselpaar generiert.

## 4.7 Zertifikatserneuerung mit Schlüsselwechsel (Re-Keying)

Bei der Zertifikatserneuerung wird immer ein neues Schlüsselpaar generiert. Dabei erfolgt stets eine Datenanpassung (siehe Kapitel 4.8).

## 4.8 Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Im Rahmen der CA for Email-Security Counterparties findet eine Zertifikatserneuerung antragsbasiert mit einem Wechsel des Schlüsselpaars und einer Anpassung von Zertifikatsinhalten sowie technischen Parametern statt.

#### 4.8.1 Gründe für eine Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Siehe CP Email-Security Certificates - Counterparties -.

#### 4.8.2 Wer kann eine Zertifikatserneuerung mit Schlüsselwechsel beantragen

Bei Zertifikaten für Geschäftspartner erfolgt die Beantragung der Zertifikatserneuerung auf Initiative von Beschäftigten der Deutschen Bundesbank bzw. der FMSA.

Siehe auchCP Email-Security Certificates - Counterparties -.

#### 4.8.3 Ablauf der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Der Prozess der Zertifikatserneuerung entspricht dem Verfahren der erstmaligen Antragstellung. Das Schlüsselpaar wird im Sicherheitsbereich der BBk-PKI im Vier-Augen-Prinzip erstellt und das Zertifikat erzeugt.

### 4.8.4 Benachrichtigung des Zertifikatsnehmers

Siehe CP Email-Security Certificates - Counterparties -.

### 4.8.5 Annahme der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Siehe CP Email-Security Certificates - Counterparties -.

### 4.8.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Siehe CP Email-Security Certificates - Counterparties -.

### 4.8.7 Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung

Siehe CP Email-Security Certificates - Counterparties -.

## 4.9 Sperrung und Suspendierung von Zertifikaten

### 4.9.1 Gründe für eine Sperrung

Siehe CP Email-Security Certificates - Counterparties -.

### 4.9.2 Wer kann eine Sperrung beantragen

Siehe CP Email-Security Certificates - Counterparties -.

### 4.9.3 Ablauf einer Sperrung

Die Sperrung eines Zertifikates kann

- per elektronischem Antragsworkflow,
- telefonisch,
- per Telefax oder
- schriftlich

erfolgen.

Die BBk-PKI führt die Sperrung des Zertifikates an der entsprechenden CA durch und veröffentlicht die entsprechende Sperrliste. Der Zertifikatsnehmer wird über die Sperrung des Zertifikates unterrichtet.

Die veröffentlichten Sperrlisten enthalten alle widerrufenen Zertifikate bis zum Ablaufdatum der entsprechenden CA.

### 4.9.4 Fristen für den Zertifikatsnehmer

Siehe CP Email-Security Certificates - Counterparties -.

### 4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Siehe CP Email-Security Certificates - Counterparties -.

### 4.9.6 Anforderung zu Sperrprüfungen durch den Zertifikatsnutzer

Siehe CP Email-Security Certificates - Counterparties -.

### 4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

CA-Sperrlisten werden mit einer Gültigkeitsdauer von 30 Tagen, Root-CA-Sperrlisten mit einer Gültigkeitsdauer von 180 Tagen ausgestellt. Eine Neuausstellung erfolgt jeweils eine Woche vor Ablauf der letzten noch gültigen Sperrliste.

Wird aufgrund einer Sperrung eines Zertifikates eine neue Sperrliste erstellt, wird diese unverzüglich veröffentlicht und ersetzt die bisher gültige Sperrliste unabhängig von deren ursprünglich angegebener Gültigkeitsdauer.

Eine neue Sperrliste enthält solange die Informationen über gesperrte Zertifikate, bis alle Zertifikate abgelaufen sind.

### 4.9.8 Maximale Latenzzeit für Sperrlisten

Siehe CP Email-Security Certificates - Counterparties -.

### 4.9.9 Online Sperrung und Statusprüfung von Zertifikaten

Nicht zutreffend. Online-Sperrungen und Statusprüfungen stehen zurzeit nicht zur Verfügung.

### 4.9.10 Anforderungen an Online Sperr- und Statusüberprüfungsverfahren

Nicht zutreffend.

### 4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Nicht zutreffend. Andere Formen zur Anzeige von Sperrinformationen werden nicht angeboten.

### 4.9.12 Kompromittierung von privaten Schlüsseln

Bei der Kompromittierung des privaten Schlüssels eines Zertifikatsnehmers ist das zugehörige Zertifikat unverzüglich zu sperren. Bei der Kompromittierung des privaten Schlüssels einer CA werden neben dem CA-Zertifikat auch alle von ihr ausgestellten Zertifikate gesperrt.

### 4.9.13 Gründe für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten ist nicht erlaubt. Einmal gesperrte Zertifikate können nicht reaktiviert werden.

### 4.9.14 Wer kann eine Suspendierung beantragen

Nicht zutreffend.

### 4.9.15 Ablauf einer Suspendierung

Nicht zutreffend.

### 4.9.16 Dauer einer Suspendierung

Nicht zutreffend.

## 4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Die BBk-PKI unterhält derzeit keinen Dienst zur Statusabfrage von Zertifikaten. Die Bereitstellung von Sperrlisten ist in Kapitel 2 geregelt.

## 4.11 Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer

Siehe CP Email-Security Certificates - Counterparties -.

## 4.12 Schlüsselhinterlegung und –wiederherstellung

Eine Schlüsselhinterlegung und –wiederherstellung durch die BBk-PKI ist technisch möglich, wird jedoch nicht angeboten.

# 5 Nicht-technische Sicherheitsmaßnahmen

## 5.1 Bauliche Sicherheitsmaßnahmen

### 5.1.1 Lage und Gebäude

Die CA for Email-Security Counterparties wird innerhalb eines zugangsgesicherten Bereiches mit einem weiteren separaten Sicherheitsbereich betrieben. Sie unterhält darüber hinaus verschiedene Tresoranlagen zur Hinterlegung von Produktiv- und Backup-Systemen und -Medien.

Der Sicherheitsbereich sowie die Tresoranlagen sind an die zentrale Alarmleitstelle des Gebäudes angebunden. Zudem ist der Sicherheitsbereich an ein lokales optisches und akustisches Alarmsystem angeschlossen.

### 5.1.2 Räumlicher Zugang

Der räumliche Zugang erfolgt über ein mehrstufiges Zugangskontrollsystem. Zu dem Sicherheitsbereich der BBk-PKI ist ausschließlich das dort produktiv tätige PKI-Betriebspersonal zutrittsberechtigt. Es wird ein ausweisbezogenes Login durchgeführt.

### 5.1.3 Stromversorgung und Klimaanlagen

Die Installation zur Stromversorgung entspricht den erforderlichen Normen. Eine Notstromversorgung über Dieselgeneratoren ist vorhanden. Eine Klimatisierung des Sicherheitsbereiches ist vorhanden.

### 5.1.4 Gefährdung durch Wasser

Die Räume verfügen über einen angemessenen Schutz vor Wasserschäden.

### 5.1.5 Brandschutz

Die Richtlinien für den Brandschutz werden eingehalten. Die Räume sind über Rauchmelder an die Brandmeldeanlage angeschlossen. Handfeuerlöscher sind in angemessener Anzahl vorhanden. Im Boden ist eine Inergen-Feuerlöschanlage installiert.

### 5.1.6 Aufbewahrung von Datenträgern

Sämtliche Datenträger mit Software sowie tagesaktuellen Sicherungen werden in mehrfachen Ausfertigungen als Original- und Backup-Versionen vorgehalten und in unterschiedlichen Gebäudeabschnitten sicher aufbewahrt. Darüber hinaus werden der Gesamtbestand außer Kraft gesetzter Software sowie alte Datensicherungen in einem Archiv hinterlegt.

Sämtliche Datenträger werden mehrstufig in anwendungsbezogenen Stahlkassetten, die sich in Tresorschränken, welche sich wiederum in Tresoranlagen befinden, sicher hinterlegt.

### 5.1.7 Abfallentsorgung

Elektronische Datenträger werden vor Ort sachgerecht geschreddert und entsorgt. Papierdatenträger werden vor Ort mittels Aktenvernichtern zerstört und sachgerecht entsorgt.

### 5.1.8 Externe Datensicherung

Eine externe Sicherung von Daten, außerhalb der BBk-PKI, bei anderen Dienstleistern findet nicht statt.

## 5.2 Organisatorische Sicherheitsmaßnahmen

### 5.2.1 Rollenkonzept

Es wird im Rahmen eines Rollenkonzeptes sichergestellt, dass einzelne Personen nicht unbemerkt Veränderungen an sicherheitskritischen Komponenten der BBk-PKI vornehmen können und Zertifikate oder private Schlüssel einsehen, generieren oder manipulieren können. Die Namen der am Prozess der Generierung sowie Auslieferung von Schlüsseln und Zertifikaten beteiligten Personen werden protokolliert.

### 5.2.2 Mehraugenprinzip

Die BBk-PKI setzt im Produktionsbetrieb für den Umgang mit hochsicherheitskritischen Zugangsmedien und kryptographischen Schlüsselmaterialien und Zertifikaten ein durchgängiges Vier-Augen-Prinzip ein.

Das Konzept sieht vor, dass die Hinterlegung, der Zugriff und der Einsatz der hochsicheren Zugangsmedien stets vom PKI-Betriebspersonal im Vier-Augen-Prinzip wahrgenommen wird. Darüber hinaus wird der gesamte Prozess der Generierung von kryptographischem Schlüsselmaterial und Zertifikaten bis zur Weitergabe im Vier-Augen-Prinzip durchgeführt. Das durchgängige Vier-Augen-Prinzip setzt die Dokumentation der Rollenverteilung der am Generierungsprozess beteiligten Personen in verschiedenen zu erstellenden sowie systembedingt erzeugten Protokollen voraus (siehe Ziffer 5.2.1).

### 5.2.3 Identifizierung und Authentifizierung für einzelne Rollen

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen umgesetzt. Die Identifizierung und Authentifizierung der Rollen erfolgt

- beim Zutritt zu Sicherheitsbereichen und Tresoren bzw.
- beim Zugriff auf Wertschränke oder sicherheitskritische Systeme und Anwendungen

mit Hilfe von SmartCards, Hardware Token, Benutzerkennungen und Passwörtern.

Die Rollenverteilung wird in verschiedenen zu erstellenden sowie systembedingt erzeugten Protokollen dokumentiert (siehe Ziffer 5.2.1).

### 5.2.4 Trennung von Rollen und Aufgaben

Das Rollenkonzept stellt die Trennung von bestimmten Rollen und Aufgaben sicher, um zu verhindern, dass eine Person allein einen Schlüssel erzeugen oder ein Zertifikat ausstellen und weitergeben kann.

## 5.3 Personelle Sicherheitsmaßnahmen

### 5.3.1 Anforderungen an PKI-Betriebspersonal

Die BBk-PKI setzt im Betrieb erfahrenes Personal ein, das über die erforderlichen IT-Kenntnisse und spezifischen Kenntnisse des CA-Betriebs verfügt.

### 5.3.2 Sicherheitsüberprüfung des PKI-Betriebspersonals

Das Personal der BBk-PKI wird von der Deutschen Bundesbank einer erweiterten Sicherheitsüberprüfung im Bereich Sabotageschutz nach dem Sicherheitsüberprüfungsgesetz (SÜG) unterzogen.

### 5.3.3 Anforderungen an Schulungen

Das mit dem Betrieb der BBk-PKI betraute Personal wird regelmäßig und anlassbezogen geschult. Es ist hinsichtlich der Sicherheitsrelevanz seiner Arbeit sensibilisiert.

### 5.3.4 Häufigkeit von Schulungen

Schulungen und Fortbildungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und IT-Verfahren durchgeführt.

### 5.3.5 Häufigkeit und Folge von Job Rotation

Das PKI-Betriebspersonal wird in allen Bereichen des CA-Betriebes eingesetzt.

### 5.3.6 Sanktionen für unerlaubte Handlungen

Unerlaubte Handlungen, die die Sicherheit der BBk-PKI gefährden oder gegen Datenschutzbestimmungen verstoßen, werden über die Personalstellen disziplinarisch geahndet bzw. strafrechtlich verfolgt.

### 5.3.7 Anforderungen an unabhängige, selbstständige Zulieferer

Nicht zutreffend.

### 5.3.8 Dokumentation für PKI-Betriebspersonal

Dem Personal der BBk-PKI stehen zum ordnungsgemäßen Betrieb der PKI folgende Dokumente zur Verfügung:

- Certificate Policy (CP),
- Certification Practice Statement (CPS),
- Betriebshandbücher,
- Benutzeranleitungen,
- Dienstvorschriften und –anweisungen.

## 5.4 Überwachungsmaßnahmen

### 5.4.1 Überwachte Ereignisse

Die nachfolgenden Ereignisse werden protokolliert und dokumentiert:

- Systeminitialisierung,
- Zertifizierungsanträge,
- Registrierung der Benutzer,
- Schlüsselerzeugung für CA, Root-CA, Benutzer,
- Zertifikatserstellung für CA, Root-CA, Benutzer,
- Datensicherungen für CA, Root-CA
- Zertifikatsveröffentlichung CA, Root-CA
- Auslieferung des privaten Schlüssels und des Zertifikates,
- Sperranträge,
- Sperrung eines Zertifikates,
- Erstellung einer Sperrliste,
- Veröffentlichung einer Sperrliste.

Darüber hinaus werden Störfälle und besondere Betriebssituationen erfasst.

### 5.4.2 Häufigkeit der Protokollanalyse

Die Ordnungsmäßigkeit des Zertifizierungsbetriebes wird im Rahmen der risikoorientierten Prüfungen des Zentralbereiches Revision der Deutschen Bundesbank vorgenommen. Bei Verdacht auf Unregelmäßigkeiten wird eine umgehende Prüfung veranlasst.

### 5.4.3 Aufbewahrungsfrist von Aufzeichnungen

Die Aufbewahrungszeiten orientieren sich an gesetzlichen Fristen, den Grundsätzen der Revisionssicherheit sowie der weiteren internen Regelungen.

### 5.4.4 Schutz von Protokolldaten

Die Protokolle werden gegen Zugriff, Manipulation und Vernichtung geschützt.

### 5.4.5 Backup der Protokolldaten

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

### 5.4.6 Überwachungssystem (intern oder extern)

Nicht zutreffend.

### 5.4.7 Benachrichtigung bei sicherheitskritischen Ereignissen

Bei Eintreten von sicherheitskritischen Ereignissen unterrichtet die BBk-PKI die zuständige Stelle für IT-Sicherheitsvorfälle und den Systemeigner.

### 5.4.8 Schwachstellenanalyse

Eine Schwachstellenanalyse kann im Bedarfsfall jederzeit durchgeführt werden.

## 5.5 Archivierung

### 5.5.1 Archivierte Daten

Sämtliche Daten, die für den Zertifizierungsprozess relevant sind (siehe Ziffer 5.4.1) werden archiviert.

### 5.5.2 Aufbewahrungsfrist für archivierte Daten

Die Aufbewahrungsfristen sind in Ziffer 5.4.3 geregelt.

### 5.5.3 Schutz der Archive

Die Archive werden gegen Zugriff, Manipulation und Vernichtung geschützt.

### 5.5.4 Datensicherungskonzept

Datensicherungen werden arbeitstäglich nach der Durchführung von

- Schlüsselausgaben,
- Sperrungen von Zertifikaten sowie
- der Erstellung von Sperrlisten

durchgeführt. Sie werden als Original- und Backupdatensicherungen vorgenommen und sicher in unterschiedlichen Gebäudebrandabschnitten hinterlegt.

### 5.5.5 Anforderungen an Zeitstempel

Eine vertrauenswürdige Zeitstempel-Quelle wird momentan nicht unterstützt.

### 5.5.6 Archivierung (intern oder extern)

Die Archivierung wird bei der betriebsverantwortlichen Stelle der BBk-PKI vorgenommen.

### 5.5.7 Verfahren zum Abruf und Überprüfen archivierter Daten

Ein standardisiertes Verfahren zum Abruf und Überprüfen archivierter Daten wird nicht angeboten.

## 5.6 Schlüsselwechsel der Zertifizierungsstelle

Ein Schlüsselwechsel der Zertifizierungsstelle erfolgt spätestens, wenn die Gültigkeit der auszustellenden Benutzerzertifikate die Restlaufzeit der CA übersteigen würde.

## 5.7 Kompromittierung und Wiederherstellung

### 5.7.1 Behandlung von Sicherheitsvorfällen und Kompromittierungen

Das Verfahren zur Behandlung von Sicherheitsvorfällen und Kompromittierungen von privaten Schlüsseln wird von der zuständigen Stelle für IT-Sicherheitsvorfälle festgelegt.

### 5.7.2 Kompromittierung bei IT-Systemen

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 Systems unverzüglich eingestellt.

Das System wird unter Verwendung der Software sowie der Datensicherungen neu aufgesetzt und nach Überprüfung in einem sicheren Zustand in Betrieb genommen. Das fehlerhafte oder modifizierte System wird analysiert. Bei Verdacht einer vorsätzlichen Handlung werden gegebenenfalls rechtliche Schritte eingeleitet.

Falls Zertifikate mit fehlerhaften Angaben generiert wurden, wird der Zertifikatsnehmer unverzüglich informiert und das Zertifikat von der Zertifizierungsstelle gesperrt.

### 5.7.3 Kompromittierung des privaten Schlüssels einer Zertifizierungsstelle

Bei Kompromittierung des privaten Schlüssels einer Zertifizierungsstelle ist das jeweilige Zertifikat sofort zu sperren. Gleichzeitig sind alle von dieser Zertifizierungsstelle ausgestellten Zertifikate der Zertifikatsnehmer zu sperren. Alle betroffenen Zertifikatsnehmer werden umgehend benachrichtigt.

Die betreffende CA wird als neue Zertifizierungsstelle mit einem neuen Schlüsselpaar aufgesetzt. Das Zertifikat der neuen Zertifizierungsstelle ist zu veröffentlichen und die zuvor gesperrten Zertifikate der Zertifikatsnehmer sind neu auszustellen.

### 5.7.4 Wiederaufnahme des Betriebs nach einer Katastrophe

Eine Wiederaufnahme des Zertifizierungsbetriebes nach einer Katastrophe ist Bestandteil der Notfallplanung und kann innerhalb kurzer Zeit erfolgen, sofern die Sicherheit des Betriebes der BBk-PKI gegeben ist.

## 5.8 Einstellung des Betriebs

Im Fall der Einstellung des Betriebes der CA for Email-Security Counterparties werden die nachfolgenden Maßnahmen ergriffen:

- Information aller Zertifikatsnehmer sowie vertrauenden Parteien mit einer Vorlauffrist von mindestens drei Monaten.
- Sperrung aller Benutzerzertifikate sowie der Zertifikate der Zertifizierungsstellen.
- Vernichtung der privaten Schlüssel der Zertifizierungsstellen.
- Veröffentlichung der entsprechenden CA- und Root-CA-Sperrlisten.

# 6 Technische Sicherheitsmaßnahmen

## 6.1 Schlüsselerzeugung und Installation

### 6.1.1 Schlüsselerzeugung

Die Schlüsselpaare der CA werden im Vier-Augen-Prinzip in einem kryptographisch gesicherten Speicher erstellt. Das IT-System wird ohne Netzwerkanschluss offline betrieben.

Die Schlüsselpaare der Zertifikatsnehmer werden zentral im Sicherheitsbereich der BBk-PKI auf IT-Systemen ohne Netzwerkanschluss offline im Vier-Augen-Prinzip erstellt.

### 6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatsnehmer

Der private Schlüssel wird dem Zertifikatsnehmer auf sicherem Weg zur Nutzung zur Verfügung gestellt. Die Zertifikatsnehmer erhalten den privaten Schlüssel mittels gesicherter elektronischer Verfahren. Nachdem der Zertifikatsnehmer den Empfang bestätigt hat wird ihm die Transport-PIN von der BBk-PKI in einem zweiten Schritt mittels gesicherter elektronischer Verfahren gegen Empfangsbestätigung bzw. telefonisch übermittelt.

### 6.1.3 Übermittlung des öffentlichen Schlüssels an den Zertifikatsaussteller

Nicht zutreffend. Eine Schlüsselerzeugung durch den Zertifikatsnehmer ist nicht vorgesehen.

### 6.1.4 Übermittlung des öffentlichen CA Schlüssels

Mit Bereitstellung des Schlüsselpaares wird ebenfalls die Zertifikatskette zur Verfügung gestellt. Die öffentlichen Schlüssel der CA können zudem über den Zertifikatsdienst gemäß Kapitel 2 abgerufen werden.

### 6.1.5 Schlüssellängen

Es werden nur Kombinationen aus Schlüsselalgorithmus und -länge verwendet, die laut Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen für eine qualifizierte elektronische Signatur nach dem Signaturgesetz als sicher eingestuft werden.

Die CA-Schlüssel der CA/Root-CA haben eine Mindestlänge von 4096 bit. Für Zertifikatsnehmer werden Schlüssel mit einer Länge von mindestens 2048 bit generiert.

### 6.1.6 Parameter der öffentlichen Schlüssel und Qualitätssicherung

Es wird folgender Verschlüsselungsalgorithmus verwendet:

- RSA mit OID 1.2.840.113549.1.1.1
- SHA1 RSA 1.2.840.113549.1.1.5 bzw. SHA256 RSA 1.2.840.113549.1.1.11

### 6.1.7 Schlüsselverwendungszwecke

Private CA-Schlüssel werden ausschließlich zum Signieren von Zertifikaten und Sperrlisten genutzt.

## 6.2 Schutz des privaten Schlüssels und Einsatz kryptographischer Module

Die privaten Schlüssel werden kryptographisch gesichert hinterlegt.

### 6.2.1 Standard kryptographischer Module

Die kryptographischen Schutzmechanismen orientieren sich an internationalen Standards. Das IT-System wird darüber hinaus ohne Netzwerkanschluss offline betrieben und außerhalb der Dienstzeiten in einer Tresoranlage aufbewahrt.

### 6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

Die privaten Schlüssel einer CA sind durch ein Vier-Augen-Prinzip geschützt.

### 6.2.3 Hinterlegung von privaten Schlüsseln (Key Escrow)

Der private CA-Schlüssel der Zertifizierungsstelle wird nicht bei Dritten hinterlegt.

### 6.2.4 Backup privater Schlüssel

Es liegt ein kryptographisch gesichertes Backup der privaten CA-Schlüssel vor. Es gelten die identischen Schutzmaßnahmen wie für das Produktivsystem. Der Zugriff erfolgt im Vier-Augen-Prinzip.

Für private Schlüssel der Zertifikatsnehmer wird kein Backup angeboten.

### 6.2.5 Archivierung privater Schlüssel

Nach Ablauf bzw. Sperrung der CA werden die privaten Schlüssel der CA noch 10 Jahre lang aufbewahrt. Es gelten die identischen Schutzmaßnahmen wie für das Produktivsystem. Der Zugriff erfolgt im Vier-Augen-Prinzip.

### 6.2.6 Transfer privater Schlüssel in oder aus einem kryptographischen Modul

Ein Transfer privater CA-Schlüssel erfolgt nur zu Backup- oder Wiederherstellungszwecken. Es gelten die identischen Schutzmaßnahmen wie für das Produktivsystem. Der Zugriff erfolgt im Vier-Augen-Prinzip.

### 6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Das Schlüsselpaar der Zertifizierungsstelle wird in einem kryptographisch gesicherten Speicher hinterlegt.

### 6.2.8 Aktivierung privater Schlüssel

Die Aktivierung des privaten CA-Schlüssels ist nur im Vier-Augen-Prinzip möglich.

Die Aktivierung des privaten Schlüssels der Zertifikatsnehmer erfolgt mit der Bestätigung des Empfangs bzw. mit der erstmaligen Nutzung des Zertifikates.

### 6.2.9 Deaktivierung privater Schlüssel

Die Deaktivierung des privaten Schlüssels einer CA erfolgt automatisch nach Beendigung des Zertifizierungsprozesses.

### 6.2.10 Vernichtung privater Schlüssel

Nach Ablauf der Gültigkeit bzw. nach Sperrung des privaten CA-Schlüssels werden diese nach einer Aufbewahrungsfrist von 10 Jahren gelöscht. Die Speichermedien werden zerstört bzw. sicher gelöscht.

### 6.2.11 Güte des kryptographischen Moduls

Siehe Ziffer 6.2.1.

## 6.3 Weitere Aspekte des Schlüsselmanagements

### 6.3.1 Archivierung öffentlicher Schlüssel

Sämtliche von der BBk-PKI erstellten öffentlichen Schlüssel werden in der Datenbank der Zertifizierungsstelle archiviert.

### 6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Die von der BBk-PKI ausgestellten Zertifikate haben folgende Gültigkeitsdauer:

- Root-CA Zertifikate maximal 12 Jahre
- CA-Zertifikate maximal 6 Jahre
- Benutzerzertifikate maximal 2 Jahre.

## 6.4 Aktivierungsdaten

Im Rahmen der BBk-PKI ist der Zugriff auf die privaten Schlüssel der Zertifizierungsstelle sowie der Benutzer kryptographisch und durch ein Vier-Augen-Prinzip geschützt.

### 6.4.1 Erzeugung und Installation der Aktivierungsdaten

Die Aktivierungsdaten werden bei der Generierung der Zertifikate erstellt. Für Passwörter und PINS's werden nicht triviale Kombinationen aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen verwendet. Die Länge muss mindestens 10 Zeichen betragen.

### 6.4.2 Schutz der Aktivierungsdaten

Die Aktivierungsdaten sind geeignet vor Verlust, Diebstahl, Veränderung, nicht autorisiertem Offenlegen sowie nicht autorisierter Verwendung geschützt.

### 6.4.3 Weitere Aspekte von Aktivierungsdaten

Nicht zutreffend.

## 6.5 Sicherheitsmaßnahmen für Computer

### 6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

Alle IT-Systeme der BBk-PKI müssen über Betriebssysteme mit aktuellen Sicherheitspatches und Virenscanner verfügen. Die BBk-PKI wird offline betrieben. Das Betriebssystem befindet sich auf einem read-only-Medium. Die Zugriffskontrolle ist als Sicherheitsmaßnahme umgesetzt.

### 6.5.2 Güte der Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen entsprechen dem aktuellen Stand der Technik. Eine Bedrohungsanalyse wurde durchgeführt sowie ein Sicherheitskonzept erstellt.

## 6.6 Technische Sicherheitsmaßnahmen während des Life Cycles

### 6.6.1 Sicherheitsmaßnahmen bei der Systementwicklung

Der Systemeigner ist in die Systementwicklung der BBk-PKI Komponenten eingebunden. Die verwendete Software hält allgemein bekannten Bedrohungsszenarien stand.

### 6.6.2 Maßnahmen im Sicherheitsmanagement

Die Betriebsstelle der BBk-PKI wurde im erhöhten Sicherheitsbedarf der Anwendung unterwiesen.

Es wird sichergestellt, dass Systementwickler keinen Zugang zur Betriebsumgebung sowie zu -daten haben.

Jegliche Veränderungen an der BBk-PKI werden einem Abnahmetestverfahren unterzogen.

### 6.6.3 Sicherheitsmaßnahmen für den gesamten Lebenszyklus

Ausgetauschte IT-Systeme oder –Komponenten werden derart außer Betrieb genommen, dass ein Funktions- und Datenmissbrauch ausgeschlossen wird. Veränderungen an den IT-Systemen oder –Komponenten werden zudem papiergebunden protokolliert.

## 6.7 Sicherheitsmaßnahmen für das Netzwerk

Die BBk-PKI wird offline betrieben. Nicht zutreffend.

## 6.8 Zeitstempel

Ein Zeitstempeldienst wird zurzeit nicht angeboten. Nicht zutreffend.

# 7 Profile von Zertifikaten, Sperrlisten und OCSP

## 7.1 Zertifikatsprofil

### 7.1.1 Versionsnummer

Von der BBk-PKI werden Zertifikate entsprechend des Standards X509v3 ausgestellt.

### 7.1.2 Zertifikatserweiterungen

CA-Zertifikate enthalten folgende Erweiterungen:

| | |
|---|---|
| **Key Usage** | cert sign, crl sign – critical |
| **Basic Constraints** | CA=true, keine Pfadlängenbeschränkung – critical |
| **Subject Alt Name** | Emailadresse – not critical |
| **Authority Key Identifier** | 160-bit SHA-1 Hash des Ausstellerschlüssels |
| **Subject Key Identifier** | 160-bit SHA-1 Hash des Ausstellerschlüssels |

Benutzerzertifikate enthalten folgende unkritische Erweiterungen:

| | |
|---|---|
| **Key Usage** | key encipherment, digital signature |
| **Extended Key Usage** | emailProtection |
| **Basic Constraints** | CA=false, keine Pfadlängenbeschränkung |
| **Subject Alt Name** | Emailadresse |
| **Issuer Alt Name** | Emailadresse |
| **Sperrlisten-Verteilpunkte** | http://www.bundesbank.de/Redaktion/DE/Downloads/Service/Services_Banken_Unternehmen/PKI/CA_for_Email-Security_Counterparties_<Ausstellungsjahr>-crl.crl?__blob=publicationFile |
| **Authority Key Identifier** | 160-bit SHA-1 Hash des Ausstellerschlüssels |
| **Subject Key Identifier** | 160-bit SHA-1 Hash des Ausstellerschlüssels |

Seriennummern werden von der austellenden Zertifizierungsstelle nicht zweimal vergeben und sind damit eindeutig.

### 7.1.3 Algorithmus Bezeichner (OID)

In den von der BBk-PKI ausgestellten Zertifikaten wird der Algorithmus
RSA (OID 1.2.840.113549.1.1.1) verwendet.

### 7.1.4 Namensformen

Die von der Root-CA ausgestellten CA-Zertifikate enthalten den kompletten DN (Distinguished Name) im Subject Name und im Issuer Name Feld.

Der Name der ausgestellten CA-Zertifikate richtet sich nach den Vorgaben des Standards x.509 und entspricht folgendem Schema:

| | |
|---|---|
| **EMAIL** | pki@bundesbank.de |
| **CN** | CA for Email-Security Counterparties <Ausstellungsjahr> |
| **OU** | SMIME-Certificates |
| **O** | Bundesbank |
| **C** | de |

Die Namen der ausgestellten Benutzerzertifikate richten sich nach den Vorgaben des Standards x.509 und entsprechen folgendem Schema:

**DN:**

| | **Geschäftspartner** |
|---|---|
| **EMAIL** | <Vorname.Name> oder <Mailstellenbezeichnung><br>@<domäne> |
| **CN** | <Vorname Name> oder <Mailstellenbezeichnung> |
| **OU** | <JJJJMMTT> |
| **OU** | CA for Email-Security Counterparties <Ausstellungsjahr> |
| **O** | <Firma> |
| **C** | de |

### 7.1.5 Namensbeschränkungen

Siehe Kapitel 3.1.

### 7.1.6 Certificate Policy Object Identifier (OID)

Die Certificate Policy OID der CP Email-Security Certificates - Counterparties - lautet: 1.3.6.1.4.1.2025.590.1.14.

### 7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkung

Nicht zutreffend.

### 7.1.8 Syntax und Semantik von Policy Qualifiern

Nicht zutreffend.

### 7.1.9 Verarbeitung und Semantik der kritischen Erweiterungen für Zertifizierungsrichtlinien

Nicht zutreffend.

## 7.2 Sperrlistenprofil

### 7.2.1 Versionsnummer

Die BBk-PKI stellt Sperrlisten gemäß der Norm x.509 in der Version 1 aus.

### 7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

In den Benutzerzertifikaten ist ein Sperrlistenverteilpunkt (CRLDP) enthalten.

## 7.3 OCSP Profil

Nicht zutreffend. OSCP wird durch die BBk-PKI zurzeit nicht unterstützt.

# 8 Konformitätsprüfung

Siehe CP Email-Security Certificates - Counterparties -.

# 9 Weitere geschäftliche und rechtliche Regelungen

Siehe CP Email-Security Certificates - Counterparties -.

# 10 Abkürzungen

| | |
|---|---|
| BBk | Deutsche Bundesbank |
| BBk-PKI | PKI der Deutschen Bundesbank |
| BSI | Bundesamt für Sicherheit in der Informationstechnologie |
| C | Country (Bestandteil des Distinguished Name) |
| CA | Certification Authority, Zertifizierungsinstanz |
| CN | Common Name (Bestandteil des Distinguished Name) |
| CP | Certificate Policy; Zertifizierungsrichtlinie einer PKI |
| CPS | Certification Practice Statement, Regelungen für den Zertifizierungsbetrieb |
| CRL | Certificate Revocation List, Sperrliste |
| CRLDP | Sperrlistenverteilpunkt |
| DN | Distinguished Name |
| DName | Distinguished Name |
| EMAIL | Email address (Bestandteil des Distinguished Name) |
| EBCA | European Bridge CA, Verknüpfung von Public-Key-Infrastrukturen einzelner Organisationen |
| FMSA | Bundesanstalt für Finanzmarktstabilisierung |
| Hardwaretoken | Hardware zur Speicherung von privaten Schlüsseln |
| HSM | Hardware Security Module |
| LDAP | Light Directory Access Protocol, Verzeichnisdienst |
| O | Organization (Bestandteil des Distinguished Name) |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| OU | Organizational Unit (Bestandteil des Distinguished Name) |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PSE | Personal Secure Environment |
| RA | Registration Authority, Registrierungsstelle |
| RFC | Request for Comment, Dokumente für weltweite Standardisierungen |
| RFC3647 | Dieser RFC dient der Beschreibung von Dokumenten, die den Betrieb einer PKI beschreiben |
| Root-CA | oberste Zertifizierungsinstanz einer PKI |
| RSA | Rivest, Shamir, Adleman |
| SHA-1 | Secure Hash Algorithm No. 1 |
| SigG | Signaturgesetz - Gesetz über Rahmenbedingungen für elektronische Signaturen |

| | |
|---|---|
| S/MIME | Secure Multipurpose Internet Mail Extensions, Standard für sichere E-Mail |
| Sperrliste | signierte Liste einer CA, die gesperrte Zertifikate enthält |
| SSL | Secure Socket Layer, Protokoll zur Transportsicherung einer Client-Server-Kommunikation |
| SÜG | Sicherheitsüberprüfungsgesetz |
| x.500 | Protokolle und Dienste für ISO konforme Verzeichnisse |
| x.509v1 | Zertifizierungsstandard |
| Zertifikat | sichere Zuordnung von öffentlichen Schlüsseln zu einem Teilnehmer |

# 11 Informationen zum Dokument

Siehe Ziffer 1.2.