DEUTSCHE BUNDESBANK
EUROSYSTEM

Certificate Policy

Email-Security Certificates - Standard -

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 Zertifizierungsrichtlinien der Deutschen Bundesbank für die Ausstellung von Zertifikaten zur Verschlüsselung sowie zur Signatur von Emails (Standard) in Form einer Certificate Policy (CP) zusammen.

Die Gliederung des Dokumentes 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:	Certificate Policy Email-Security Certificates - Standard -
Version:	1.0
Datum:	15.02.2016
OID:	1.3.6.1.4.1.2025.590.1.13

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 nachgeordneten CA's werden verwendet, um Benutzerzertifikate 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

- Beschäftigte der Deutschen Bundesbank,
- Beschäftigte der Bundesanstalt für Finanzmarktstabilisierung (FMSA) sowie
- bei Bedarf deren jeweilige externe Mitarbeiterinnen und Mitarbeiter.

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

Die ausgestellten Zertifikate dürfen nur zur Verschlüsselung sowie zur Signatur von Emails (Standard) in Zusammenhang mit Geschäftsangelegenheiten der Deutschen Bundesbank bzw. der FMSA verwendet werden.

1.4.2 Verbotene Verwendungen von Zertifikaten

Die private Verwendung der Zertifikate ist untersagt.

1.5 Verwaltung der Zertifizierungsrichtlinien

1.5.1 Zuständigkeit für das Dokument

Diese CP 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.demailto:

1.5.3 Prüfung der Zertifizierungsrichtlinie

Diese CP wird durch den Systemeigner der BBk-PKI überprüft.

Der Systemeigner der BBk-PKI stellt die Übereinstimmung der CPS mit den Vorgaben der jeweiligen CP sicher.

1.5.4 Veröffentlichung der Richtlinie

Diese CP 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 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

Anonymität oder Pseudonymität in Namen von Zertifikaten ist nicht erlaubt.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

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

Zudem gelten die Lotus Notes/Domino Namenskonventionen der Deutschen Bundesbank.

3.1.5 Eindeutigkeit von Namen

Die Eindeutigkeit von Namen und E-Mailadresse wird von der BBk-PKI gewährleistet. Darüber hinaus wird jedem Zertifikat eine eindeutige Seriennummer zugeordnet, welche eine eindeutige und unveränderliche Zuordnung zum Zertifikatsnehmer ermöglicht.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Die BBk-PKI bietet grundsätzlich keine Prozeduren zur Auflösung von Markenstreitigkeiten an. Diese sind zwischen den daran beteiligten Unternehmen ggf. durch markenrechtliche oder wettbewerbsrechtliche Maßnahmen im Zivilrechtsweg zu lösen.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Die Schlüsselpaare der Zertifizierungsstellen und der Zertifikatsnehmer werden ausschließlich durch die BBk-PKI generiert.

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

Sämtliche Beschäftigte der Deutschen Bundesbank sowie der FMSA und deren jeweilige externe Mitarbeiterinnen und Mitarbeiter werden grundsätzlich von den zuständigen Personalstellen persönlich (face-to-face) registriert.

Der Registrierungsprozess für die Nutzung von Zertifikaten zur Verschlüsselung sowie zur Signatur von Emails (Standard) besteht aus einem mehrstufigen Verfahren. Die Beantragung eines Zertifikates erfogt über einen elektronischen Antragsworkflow, der nach Genehmigung durch den direkten Vorgesetzten des Antragstellers an die BBK-PKI übersendet wird.

Die Authentifizierung des Zertifikatsinhabers erfolgt gemäß dem nachfolgenden Prozess:

- Ein neuer Mitarbeiter muss sich in der Personalabteilung mittels eines Personalausweises oder Reisepasses identifizieren, um einen Dienstausweis zu erhalten.
- Der Dienstausweis ist Voraussetzung zur Beantragung einer eindeutigen Benutzer-ID sowie eines Kennwortes zur Nutzung des internen Netzwerkes.
- Erst danach ist der Benutzer in der Lage eine Email-Berechtigung zu beantragen.
- Mit dem Netzwerkzugang sowie der Email-Berechtigung kann der Benutzer dann einen elektronischen Workflow zur Beantragung eines Zertifikates starten.

Für jede Zertifikatsbeantragung (Erstantrag und Erneuerung) ist die Genehmigung des direkten Vorgesetzten erforderlich, der seine Mitarbeiter persönlich (face-to-face) kennt.

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

Diese Prüfung wird im jeweiligen CPS beschrieben.

3.2.6 Kriterien für Cross-Zertifizierung und Interoperabilität

Nicht zutreffend. Eine Cross-Zertifizierung mit anderen Organisationen ist derzeit nicht geplant.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Die Zertifikatsnehmer werden vor Ablauf der Gültigkeit des Zertifikates mehrfach zur Zertifikatserneuerung aufgefordert.

Die Identifizierung und Authentifizierung erfolgt analog zum initialen Antragsprozess.

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 Identität des Antragstellers bei Sperranträgen wird 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

Zertifikate können von den in Ziffer 1.3.3 benannten Zertifikatsnehmern beantragt werden.

4.1.2 Registrierungsprozess und Zuständigkeit

Die Beantragung von Zertifikaten erfolgt im Rahmen eines mehrstufigen Registrierungsprozesses an die BBk-PKI. Dabei werden folgende Prüfungen vorgenommen:

- Berechtigung des Antragstellers,
- Vollständigkeit und Korrektheit des Antrags,
- Eindeutigkeit des DN,
- Prüfung der Authentizität von Personen bzw. Organisationen.

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

Trotz Erfüllung der formalen Voraussetzungen besteht kein Anspruch auf Erteilung eines Zertifikats. Die BBk-PKI bleibt in ihrer Vergabeentscheidung frei.

4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

Die Bearbeitungsdauer von Zertifikatsanträgen beträgt grundsätzlich maximal eine Woche.

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.

4.3.2 Benachrichtigung des Zertifikatsnehmers

Der Zertifikatsnehmer wird von der BBk-PKI über die Ausstellung des Zertifikates informiert.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Die Annahme des Zertifikates erfolgt mit der Bestätigung des Empfangs bzw. mit der Nutzung des Zertifikats.

4.4.2 Veröffentlichung des Zertifikats

Eine Veröffentlichung der Zertifikate in einem Verzeichnisdienst wird nicht ausgeschlossen.

4.4.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist nicht erforderlich.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die Nutzung des privaten Schlüssels ist ausschließlich dem Zertifikatsnehmer vorbehalten.

Der Zertifikatsnehmer hat insbesondere die Aufgaben

- unverzüglich anzuzeigen, falls die Angaben in seinem Zertifikat nicht oder nicht mehr den Tatsachen entsprechen,
- die Beschränkungen hinsichtlich der Verwendung seines privaten Schlüssels einzuhalten (siehe Ziffer 1.4.1),
- unverzüglich die Sperrung des Zertifikates zu veranlassen, wenn sein privater Schlüssel kompromittiert ist oder das Zertifikat nicht länger benötigt wird (siehe Kapitel 4.9).

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikats durch den Zertifikatsnutzer

Zertifikatsnutzer sind IT-Systeme oder IT-Prozesse, die das Zertifikat nur für die im Zertifikat ausgewiesenen Verwendungszwecke einsetzen. Darüber hinaus überprüfen sie die Gültigkeitsdauer des Zertifikates.

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 BBk-PKI 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

Die nachfolgenden Gründe führen zu einer Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung:

- Routinemäßige Zertifikatserneuerung
  - bei bevorstehendem Ablauf der Gültigkeit des Zertifikates oder
  - bereits erfolgtem Ablauf der Gültigkeit des Zertifikates.
- Zertifikatsbeantragung nach einer Sperrung des bisherigen Zertifikates.
- Die Daten des Zertifikates entsprechen nicht oder nicht mehr den Tatsachen.
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des Zertifikates bieten keine ausreichende Sicherheit mehr oder eine Erneuerung der Zertifikatsstruktur ist zwingend erforderlich.

4.8.2 Wer kann eine Zertifikatserneuerung mit Schlüsselwechsel beantragen

Die Zertifikatserneuerung wird vom Zertifikatsnehmer beantragt.Falls die Schlüssellänge, die Gültigkeitsdauer oder die Zertifikatsstruktur aus Sicherheitsgründen außerplanmäßig die Erneuerung von Zertifikaten erforderlich machen sollte, wird die Zertifikatserneuerung von der BBk-PKI ohne ein vorheriges Antragsverfahren durchgeführt. Die Zertifikatsnehmer werden über die erfolgte außerplanmäßige Zertifikatserneuerung informiert.

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

Nach Erstellung wird das Zertifikat dem Zertifikatsnehmer in geeigneter Weise durch die BBk-PKI sicher übermittelt oder der Zertifikatsnehmer über dessen Ausstellung informiert.

4.8.5 Annahme der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Die Annahme des Zertifikates erfolgt mit der Bestätigung des Empfangs bzw. mit der Nutzung des Zertifikates.

4.8.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Eine Veröffentlichung der Zertifikate in einem Verzeichnisdienst wird nicht ausgeschlossen.

4.8.7 Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung

Eine Benachrichtigung weiterer Instanzen ist nicht erforderlich.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für eine Sperrung

Ein Zertifikat muss gesperrt werden, wenn mindestens einer der folgenden Gründe eintritt:

- Die im Zertifikat enthaltenen Angaben sind nicht oder nicht mehr gültig.
- Der private Schlüssel wurde kompromittiert.
- Der Zertifikatsnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr.
- Der Zertifikatsnehmer hält Verpflichtungen gemäß dieses CP bzw. des CPS nicht ein (siehe Ziffer 4.5).
- Die BBk-PKI stellt ihren Zertifizierungsbetrieb ein. In diesem Fall werden sämtliche von der BBk-PKI ausgestellten Zertifikate gesperrt.
- Der private Schlüssel der ausstellenden oder einer übergeordneten Root-CA wird kompromittiert. In diesem Fall werden sämtliche von diesen CA's ausgestellte Zertifikate gesperrt.
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des Zertifikates bieten keine ausreichende Sicherheit mehr. Die BBk-PKI behält sich vor, die betreffenden Zertifikate zu sperren.

4.9.2 Wer kann eine Sperrung beantragen

Die Sperrung eines Zertifikates kann vom Zertifikatsnehmer, einem vom Zertifikatsnehmer Beauftragten oder vom Vorgesetzten beauftragt werden.

Personen, die die Identität bzw. Berechtigung eines Zertifikatsnehmers bei der Beantragung des Zertifikats bestätigt haben, können ebenfalls jederzeit die Sperrung beantragen, wenn der Zertifikatsnehmer nicht mehr berechtigt ist, das Zertifikat zu nutzen.

Der Benutzer kann die Sperrung seines eigenen Zertifikates jederzeit beantragen, auch wenn keiner der in Ziffer 4.9.1 genannten Gründe vorliegt.

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.

4.9.4 Fristen für den Zertifikatsnehmer

Die Zertifikatsnehmer sind verpflichtet, bei bekannt werden eines Sperrgrundes unverzüglich die Sperrung des Zertifikates zu veranlassen.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Die Sperrung des Zertifikates wird von der BBk-PKI unverzüglich nach Zugang des Sperrantrages durchgeführt. Nachdem der Sperrantrag gestellt wurde, wird die Sperrung selbst innerhalb von 24 Stunden durchgeführt. An Werktagen (Montag bis Freitag) ist die Organisationeinheit PKI Services für die Sperrbearbeitung verantwortlich. Am Wochenende kann die Sperrung von Zertifikaten über den Fist-Level-Support beantragt werden.

4.9.6 Anforderung zu Sperrprüfungen durch den Zertifikatsnutzer

Sperrinformationen werden mittels Sperrlisten veröffentlicht. Zur Prüfung der Gültigkeit von Zertifikaten muss der Zertifikatsnutzer jeweils die aktuell veröffentlichte Sperrliste verwenden.

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

Die Veröffentlichung von Sperrlisten wird unmittelbar nach deren Erzeugung veranlasst.

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

Eine Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer erfolgt entweder durch die Sperrung des Zertifikates oder indem nach Ablauf der Gültigkeit kein neues Zertifikat beantragt wird.

4.12 Schlüsselhinterlegung und –wiederherstellung

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

5 Nicht-technische Sicherheitsmaßnahmen

Detaillierte Informationen finden sich in den entsprechenden CPS.

6 Technische Sicherheitsmaßnahmen

Detaillierte Informationen finden sich in den entsprechenden CPS.

7 Profile von Zertifikaten, Sperrlisten und OCSP

Detaillierte Informationen finden sich in den entsprechenden CPS.

8 Konformitätsprüfung

Die Arbeitsprozesse der Zertifizierungsstelle sowie der an der Registrierung beteiligten Stellen werden regelmäßig bzw. anlassbezogen überprüft.

Die Audits des technischen Aufbaus der PKI und der operativen Abläufe werden in regelmäßigen Abständen durch die interne Revision nach den in der Deutschen Bundesbank für solche Vorgänge festgelegten Regeln durchgeführt. Die Ergebnisse der Audits werden nicht veröffentlicht.

8.1 Frequenz und Umstände der Überprüfung

Grundsätzlich werden interne Audits und Prüfungen in regelmäßigen Abständen vorgenommen.

8.2 Identität und Qualifikation des Überprüfers

Die internen Prüfungen werden durch den Zentralbereich Revision, durch den Systemeigner sowie die Leitung der BBk-PKI vorgenommen. Die Prüfer verfügen über das Know-how sowie die notwendigen Kenntnisse auf dem Gebiet Public Key Infrastructure (PKI), um die Prüfungen vornehmen zu können.

8.3 Verhältnis von Prüfer zu Überprüftem

Der Prüfer darf nicht in den Produktionsprozess der BBk-PKI eingebunden sein. Eine Selbstüberprüfung ist nicht erlaubt.

8.4 Überprüfte Bereiche

Es können alle für die PKI relevanten Bereiche überprüft werden. Die Prüfungsinhalte obliegen dem Prüfer.

8.5 Mängelbeseitigung

Festgestellte Mängel müssen in Abstimmung zwischen Zertifizierungsstelle und Prüfer zeitnah beseitigt werden. Der Prüfer wird über die Beseitigung der Mängel informiert.

8.6 Veröffentlichung der Ergebnisse

Eine Veröffentlichung der Prüfungsergebnisse ist nicht vorgesehen.

9 Weitere geschäftliche und rechtliche Regelungen

9.1 Gebühren

Es werden keine Gebühren erhoben.

9.2 Finanzielle Verantwortung

Risiken, die aus der Haftung für eine CA entstehen können, werden durch Deutsche Bundesbank abgedeckt.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Alle Informationen und Daten über Zertifikatsnehmer und Teilnehmer der BBk-PKI, die nicht unter Ziffer 9.3.2 fallen, werden als vertrauliche Informationen eingestuft.

9.3.2 Nicht vertraulich zu behandelnde Daten

Alle Informationen und Daten, die in herausgegebenen Zertifikaten und Sperrlisten 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

Die BBk-PKI trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

9.4 Schutz personenbezogener Daten

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

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

9.4.2 Vertraulich zu behandelnde Daten

Jegliche Daten über Zertifikatsnehmer und Teilnehmer der BBk-PKI werden vertraulich behandelt.

9.4.3 Nicht vertraulich zu behandelnde Daten

Es gelten die Bestimmungen in Ziffer 9.3.2.

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Die BBk-PKI trägt die Verantwortung für Maßnahmen zum Schutz personenbezogener Daten.

9.4.5 Nutzung personenbezogener Daten

Der Zertifikatsnehmer stimmt der Nutzung von personenbezogenen Daten durch die BBk-PKI 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 im Rahmen einer gerichtlichen Beweisführung

Die BBk-PKI richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten nach den gesetzlichen Datenschutzbestimmungen. Eine Offenlegung findet gegenüber staatlichen Instanzen nur bei Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen statt.

9.4.7 Andere Umstände einer Veröffentlichung

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

9.5 Urheberrechte

Die Deutsche Bundesbank ist Urheber dieses Dokumentes. Das Dokument kann unverändert an Dritte weitergegeben werden.

9.6 Verpflichtungen

9.6.1 Verpflichtung der Zertifizierungsstellen

Die BBk-PKI verpflichtet sich, den Bestimmungen dieser CP zu folgen.

9.6.2 Verpflichtung der Registrierungsstellen

Die BBk-PKI sowie die in die Registrierung eingebundenen Stellen verpflichten sich, den Bestimmungen dieser CP zu folgen.

9.6.3 Verpflichtung des Zertifikatsnehmers

Die Verpflichtung des Zertifikatsnehmers ist in Ziffer 4.5.1 geregelt.

9.6.4 Verpflichtung des Zertifikatsnutzers

Die Verpflichtung des Zertifikatsnutzers ist in Ziffer 4.5.2 geregelt. Darüber hinaus muss er den Zertifikatsrichtlinien seiner Organisation folgen.

9.6.5 Verpflichtung anderer Teilnehmer

Von der BBk-PKI beauftragte Dienstleister (z. B. Betreiber von Verzeichnisdiensten) werden auf die Einhaltung dieser CP verpflichtet.

9.7 Gewährleistung

Grundsätzlich wird keine Gewährleistung übernommen. Die Deutsche Bundesbank garantiert nicht die Verfügbarkeit der Leistungen der PKI.

9.8 Haftungsbeschränkung

Verletzt die Deutsche Bundesbank bei der Vertragsdurchführung schuldhaft eine vertragswesentliche Pflicht, die hierfür im Einzelfall von besonderer Bedeutung ist, so haftet sie für den dadurch entstehenden Schaden. Bei einfacher Fahrlässigkeit ist die Haftung der Deutschen Bundesbank auf den vertragstypischen Schaden beschränkt.

Für die Verletzung sonstiger Pflichten haftet die Deutsche Bundesbank nur bei grobem Verschulden. Gegenüber Kaufleuten und öffentlichen Verwaltungen gilt die Haftungsbeschränkung des Absatz 1 Satz 2 auch bei grober Fahrlässigkeit einfacher Erfüllungsgehilfen.

Vorstehende Haftungsausschlüsse und –begrenzungen finden keine Anwendung auf die Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit; insofern haftet die Deutsche Bundesbank nach den gesetzlichen Bestimmungen.

Im Falle einer Haftung der Deutschen Bundesbank nach den vorstehenden Absätzen bestimmt sich der Haftungsumfang entsprechend § 254 BGB danach, wie das Verschulden der Deutschen Bundesbank im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt hat.

9.9 Haftungsfreistellung

Bei der unsachgemäßen Verwendung des Zertifikats und dem zugehörigen privaten Schlüssel oder einer Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung ist die Deutsche Bundesbank von der Haftung freigestellt.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Diese CP tritt an dem Tag in Kraft, an dem es gemäß Kapitel 2 veröffentlicht wird.

9.10.2 Aufhebung

Dieses Dokument ist so lange gültig, bis es durch eine neue Version ersetzt wird oder der Betrieb der BBk-PKI eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Von den Konsequenzen der Aufhebung diese CP bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten unberührt.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

In dieser Zertifizierungsrichtlinie werden keine entsprechenden Regelungen getroffen.

9.12 Änderungen der Richtlinie

9.12.1 Vorgehen bei Änderungen

Änderungen der CP werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht.

9.12.2 Benachrichtigungsmethode und –fristen

Die Zertifikatsnehmer werden rechtzeitig vor dem Inkrafttreten auf die Änderung der CP per signierter E-Mail hingewiesen.

Beschäftigten der Deutschen Bundesbank, der FMSA sowie deren externen Mitarbeiterinnen und Mitarbeitern gegenüber gilt die im Intranet bekannt gemachte jeweils aktuelle Fassung der CP.

9.12.3 Bedingungen für die Änderung des Richtlinienbezeichners (OID)

Der Richtlinienbezeichner ändert sich bis zum Ende der Gültigkeit der zugehörigen Zertifizierungsinstanz nicht.

9.13 Schiedsverfahren

Die Anrufung eines Schiedsverfahrens liegt im Ermessen der Deutschen Bundesbank.

9.14 Gerichtsstand

Der Gerichtsstand ist Frankfurt am Main.

9.15 Konformität mit geltendem Recht

Es gilt deutsches Recht. Die von der BBk-PKI ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten gemäß Signaturgesetz.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Alle Regelungen in dieser CP gelten zwischen der BBk-PKI und den Zertifikatsnehmern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Abtretung der Rechte

Eine Abtretung von Rechten ist nicht vorgesehen.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Zertifizierungsrichtlinie unwirksam sein oder werden, so lässt dies den übrigen Inhalt der Zertifizierungsrichtlinie unberührt. Auch eine Lücke berührt nicht die Wirksamkeit der Zertifizierungsrichtlinie im Übrigen. Anstelle der unwirksamen Bestimmung gilt diejenige wirksame Bestimmung als vereinbart, welche der ursprünglich gewollten am nächsten kommt oder nach Sinn und Zweck der Zertifizierungsrichtlinie geregelt worden wäre, sofern der Punkt bedacht worden wäre.

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

Rechtliche Auseinandersetzungen, die aus dem Betrieb der BBk-PKI herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland.

Erfüllungsort und Gerichtsstand ist Frankfurt am Main.

9.16.5 Höhere Gewalt

Die Deutsche Bundesbank übernimmt keine Haftung für die Verletzung einer Pflicht sowie für Verzug oder Nichterfüllung im Rahmen dieser CP, sofern das zugrunde liegende Ereignis außerhalb ihrer Kontrolle (z. B. höhere Gewalt, Kriegshandlungen, Netzausfälle, Brände, Erdbeben und andere Katastrophen) resultiert.

9.17 Andere Regelungen

Nicht zutreffend.

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	Secure Hash Algorithm
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.