

# **TeleTrust EBCA**

*European Bridge Certificate Authority*

## **Certificate Policy**

für Teilnehmer der  
TeleTrust European Bridge CA

## Informationen zum Dokument

Version 2.3

28.06.2016

TeleTrusT – Bundesverband IT-Sicherheit e.V.  
 Chausseestraße 17  
 D-10115 Berlin

Tel. +49 30 / 400 54 310  
 Fax +49 30 / 400 54 311

info@ebca.de  
<http://www.ebca.de>

## Historie

Ver- sion	Datum	Änderung	Autor
1.08	11.01.2012	Anpassung des Verbandsnamens	Dr. Holger Mühlbauer
1.09	08.02.2012	Anpassung Erscheinung, Anpassung Begrifflichkeiten	Marieke Petersohn
1.10	21.01.2014	Vorbereitung zur Überarbeitung am 27.01.2014	Dr. Willi Kafitz
1.11	27.01.2014	Überarbeitung	Wolfgang Siegert/ Michael Thiel/ Dr. Frank Losemann/ Dr. Willi Kafitz/ Marieke Petersohn/ Martin Fuhrmann
1.12	14.02.2014	Überarbeitung	Dr. Willi Kafitz/ Martin Fuhrmann
1.13	21.03.2014	Überarbeitung Glossar	Wolfgang Siegert/ Willi Kafitz/ Martin Fuhrmann
1.14	03.04.2014	Überarbeitung	Martin Fuhrmann
1.15	16.04.2014	Überarbeitung	Martin Fuhrmann
2.0	22.04.2014	Beschlussfassung, Anpassung Datum und Versionsnummer	Martin Fuhrmann
2.1	12.06.2014	Fehlerbeseitigung Glossar	Martin Fuhrmann
2.2	17.07.2014	Neues EBCA-Logo eingefügt	Martin Fuhrmann
2.3	28.06.2016	Änderungen der Bestimmungen zum Ort der PKI	Marieke Petersohn

# Inhaltsübersicht

<b>1</b>	<b>Einleitung</b>	<b>8</b>
1.1	Überblick	8
1.1.1	Ziel dieser Richtlinie	8
1.1.2	RFC 3647 Struktur	8
1.1.3	Konventionen	9
1.1.4	Gültigkeit	9
1.2	Name und Kennzeichnung des Dokuments	9
1.3	PKI-Teilnehmer	9
1.3.1	Zertifizierungsstellen (Certification Authorities)	9
1.3.2	Registrierungsstellen (Registration Authorities)	9
1.3.3	Zertifikatsnehmer	9
1.3.4	Zertifikatsnutzer	10
1.3.5	Andere Teilnehmer	10
1.4	Verwendung von Zertifikaten	10
1.4.1	Erlaubte Verwendungen von Zertifikaten	10
1.4.2	Verbotene Verwendungen von Zertifikaten	10
1.5	Pflege der Richtlinie	10
1.5.1	Zuständigkeit für das Dokument	10
1.5.2	Ansprechpartner/Kontaktperson/Sekretariat	10
1.5.3	Pflege dieser Richtlinie	10
1.5.4	Annahmeverfahren für Teilnehmer-CP	10
1.5.5	Zuständiger für die Anerkennung einer CP in Hinblick auf diese CP	11
1.6	Begriffe und Abkürzungen	11
1.6.1	Deutsche Begriffe siehe Glossar	11
1.6.2	Englische Begriffe siehe Glossar	11
1.6.3	Abkürzungen siehe Glossar	11
1.6.4	Referenzen	11
<b>2</b>	<b>Verantwortlichkeit für Verzeichnisse und Veröffentlichungen</b>	<b>12</b>
2.1	Verzeichnisse	12
2.2	Veröffentlichung von Informationen zur Zertifikatserstellung	12
2.3	Zeitpunkt und Häufigkeit von Veröffentlichungen	12
2.4	Zugriffskontrollen auf Verzeichnisse	12
<b>3</b>	<b>Identifizierung und Authentifizierung</b>	<b>13</b>
3.1	Namensregeln	13
3.1.1	Arten von Namen	13
3.1.2	Notwendigkeit für aussagefähige Namen	13
3.1.3	Anonymität oder Pseudonymität von Zertifikatsnehmern	13
3.1.4	Regeln für die Interpretation verschiedener Namensformen	13
3.1.5	Eindeutigkeit von Namen	13
3.1.6	Anerkennung, Authentifizierung und Rolle von Markennamen	13
3.2	Erstmalige Überprüfung der Identität	13
3.2.1	Methoden zur Überprüfung des Besitzes des privaten Schlüssels	13
3.2.2	Authentifizierung von Organisationszugehörigkeiten	13
3.2.3	Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers	13
3.2.4	Ungeprüfte Zertifikatsnehmerangaben	13
3.2.5	Prüfung der Berechtigung zur Antragstellung	13
3.2.6	Kriterien zur "Interoperation" (Zusammenwirkung/Wechselwirkung)	13
3.3	Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Rekeying)	14
3.3.1	Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung	14
3.3.2	Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen	14
3.4	Identifizierung und Authentifizierung von Sperranträgen	14
<b>4</b>	<b>Betriebsanforderungen</b>	<b>15</b>
4.1	Zertifikatsantrag	15
4.1.1	Wer kann einen Zertifikatsantrag stellen?	15
4.1.2	Registrierungsprozess und Zuständigkeiten	15
4.2	Verarbeitung des Zertifikatsantrags	15

4.2.1	Durchführung der Identifizierung und Authentifizierung .....	15
4.2.2	Annahme oder Ablehnung von Zertifikatsanträgen .....	15
4.2.3	Fristen für die Bearbeitung von Zertifikatsanträgen .....	15
4.3	Zertifikatsausgabe .....	15
4.3.1	Aktionen des Zertifizierungsdiensteanbieters (Trust Service Provider) bei der Ausgabe von Zertifikaten .....	15
4.3.2	Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats durch die CA .....	15
4.4	Zertifikatsannahme .....	15
4.4.1	Verhalten für eine Zertifikatsannahme .....	15
4.4.2	Veröffentlichung des Zertifikats durch die CA .....	15
4.4.3	Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats .....	15
4.5	Verwendung des Schlüsselpaares und des Zertifikats.....	16
4.5.1	Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer.....	16
4.5.2	Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer .....	16
4.6	Zertifikatserneuerung.....	16
4.6.1	Bedingungen für eine Zertifikatserneuerung .....	16
4.6.2	Wer darf eine Zertifikatserneuerung beantragen?.....	16
4.6.3	Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung .....	16
4.6.4	Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats .....	16
4.6.5	Verhalten für die Annahme einer Zertifikatserneuerung .....	16
4.6.6	Veröffentlichung der Zertifikatserneuerung durch die CA .....	16
4.6.7	Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats.....	16
4.7	Zertifizierung nach Schlüsselerneuerung .....	16
4.7.1	Bedingungen für eine Zertifizierung nach Schlüsselerneuerung.....	16
4.7.2	Wer darf Zertifikate für Schlüsselerneuerungen beantragen? .....	17
4.7.3	Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen .....	17
4.7.4	Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats .....	17
4.7.5	Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen.....	17
4.7.6	Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA.....	17
4.7.7	Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats .....	17
4.8	Zertifikatsänderung .....	17
4.8.1	Bedingungen für eine Zertifikatsänderung .....	17
4.8.2	Wer darf eine Zertifikatsänderung beantragen?.....	17
4.8.3	Bearbeitung eines Antrags auf Zertifikatsänderung .....	17
4.8.4	Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats .....	17
4.8.5	Verhalten für die Annahme einer Zertifikatsänderung.....	17
4.8.6	Veröffentlichung der Zertifikatsänderung durch die CA .....	17
4.8.7	Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines neuen Zertifikats .....	17
4.9	Sperrung und Suspendierung von Zertifikaten.....	17
4.9.1	Bedingungen für eine Sperrung.....	17
4.9.2	Wer kann eine Sperrung beantragen? .....	18
4.9.3	Verfahren für einen Sperrantrag.....	18
4.9.4	Fristen für einen Sperrantrag.....	18
4.9.5	Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch den Zertifizierungsdiensteanbieter (Trust Service Provider) .....	18
4.9.6	Verfügbare Methoden zum Prüfen von Sperrinformationen.....	18
4.9.7	Frequenz der Veröffentlichung von Sperrlisten .....	18
4.9.8	Maximale Latenzzeit für Sperrlisten .....	18
4.9.9	Verfügbarkeit von Online-Sperrinformationen .....	18
4.9.10	Anforderungen zur Online-Prüfung von Sperrinformationen.....	18
4.9.11	Andere Formen zur Anzeige von Sperrinformationen .....	18
4.9.12	Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels.....	18
4.9.13	Bedingungen für eine Suspendierung .....	18
4.9.14	Wer kann eine Suspendierung beantragen? .....	18
4.9.15	Verfahren für Anträge auf Suspendierung.....	18
4.9.16	Begrenzungen für die Dauer von Suspendierungen .....	18
4.10	Statusabfragedienst für Zertifikate .....	19
4.10.1	Funktionsweise des Statusabfragedienstes .....	19
4.10.2	Verfügbarkeit des Statusabfragedienstes .....	19

4.10.3	Optionale Leistungen.....	19
4.11	Kündigung durch den Zertifikatsnehmer .....	19
4.12	Schlüsselhinterlegung und Wiederherstellung .....	19
4.12.1	Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel .	19
4.12.2	Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln .....	19
<b>5</b>	<b>Nicht-technische Sicherheitsmaßnahmen .....</b>	<b>20</b>
5.1	Bauliche Sicherheitsmaßnahmen .....	20
5.1.1	Lage und Gebäude .....	20
5.1.2	Zugang.....	20
5.1.3	Strom, Heizung und Klimaanlage .....	20
5.1.4	Wassergefährdung .....	20
5.1.5	Brandschutz.....	20
5.1.6	Lager und Archiv .....	20
5.1.7	Müllbeseitigung.....	20
5.1.8	Desaster Backup .....	20
5.2	Verfahrensvorschriften.....	20
5.2.1	Rollenkonzept .....	20
5.2.2	Mehraugenprinzip .....	20
5.2.3	Rollenausschlüsse.....	20
5.2.4	Rollentrennung .....	20
5.3	Personalkontrolle .....	21
5.3.1	Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit.....	21
5.3.2	Methoden zur Überprüfung der Rahmenbedingungen.....	21
5.3.3	Anforderungen an Schulungen.....	21
5.3.4	Häufigkeit von Schulungen und Belehrungen .....	21
5.3.5	Häufigkeit und Folge von Job-Rotation .....	21
5.3.6	Maßnahmen bei unerlaubten Handlungen .....	21
5.3.7	Anforderungen an freie Mitarbeiter.....	21
5.3.8	Dokumente, die dem Personal zur Verfügung gestellt werden müssen .....	21
5.4	Überwachungsmaßnahmen .....	21
5.4.1	Arten von aufgezeichneten Ereignissen.....	21
5.4.2	Häufigkeit der Bearbeitung der Aufzeichnungen.....	21
5.4.3	Aufbewahrungszeit von Aufzeichnungen .....	21
5.4.4	Sicherung der Aufzeichnungen .....	21
5.4.5	Datensicherung der Aufzeichnungen .....	21
5.4.6	Speicherung der Aufzeichnungen (intern/extern).....	21
5.4.7	Benachrichtigung der Ereignisauslöser .....	21
5.4.8	Verwundbarkeitsabschätzungen .....	21
5.5	Archivierung von Aufzeichnungen .....	21
5.5.1	Arten von archivierten Aufzeichnungen.....	21
5.5.2	Aufbewahrungsfristen für archivierte Daten .....	21
5.5.3	Sicherung des Archivs.....	22
5.5.4	Datensicherung des Archivs.....	22
5.5.5	Anforderungen zum Zeitstempeln von Aufzeichnungen .....	22
5.5.6	Archivierung (intern/extern) .....	22
5.5.7	Verfahren zur Beschaffung und Verifikation von Archivinformationen.....	22
5.6	Schlüsselwechsel beim Zertifizierungsdiensteanbieter (Trust Service Provider).....	22
5.7	Kompromittierung und Geschäftweiterführung beim Zertifizierungsdiensteanbieter (Trust Service Provider) .....	22
5.7.1	Behandlung von Vorfällen und Kompromittierungen.....	22
5.7.2	Rechnerressourcen-, Software- und/oder Datenkompromittierung.....	22
5.7.3	Verhalten bei Kompromittierung des privaten Schlüssels des Zertifizierungsdiensteanbieters (Trust Service Providers).....	22
5.7.4	Möglichkeiten zur Geschäftweiterführung nach einer Kompromittierung.....	22
5.8	Schließung eines Zertifizierungsdiensteanbieters (Trust Service Providers) oder einer Registrierungsstelle (Registration Authority) .....	22
<b>6</b>	<b>Technische Sicherheitsmaßnahmen .....</b>	<b>23</b>
6.1	Erzeugung und Installation von Schlüsselpaaren .....	23

6.1.1	Erzeugung von Schlüsselpaaren.....	23
6.1.2	Lieferung privater Schlüssel an Zertifikatsnehmer .....	23
6.1.3	Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber .....	23
6.1.4	Lieferung öffentlicher Schlüssel des Zertifizierungsdiensteanbieter (Trust Service Provider) an Zertifikatsnutzer .....	23
6.1.5	Schlüssellängen .....	23
6.1.6	Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle .....	23
6.1.7	Schlüsselverwendungen.....	23
6.2	Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module .....	23
6.2.1	Standards und Sicherheitsmaßnahmen für kryptographische Module .....	23
6.2.2	Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m) .....	23
6.2.3	Hinterlegung privater Schlüssel.....	23
6.2.4	Sicherung privater Schlüssel .....	23
6.2.5	Archivierung privater Schlüssel .....	23
6.2.6	Transfer privater Schlüssel in oder aus kryptographischen Modulen .....	24
6.2.7	Speicherung privater Schlüssel in kryptographischen Modulen.....	24
6.2.8	Aktivierung privater Schlüssel .....	24
6.2.9	Deaktivierung privater Schlüssel .....	24
6.2.10	Zerstörung privater Schlüssel.....	24
6.2.11	Beurteilung kryptographischer Module .....	24
6.3	Andere Aspekte des Managements von Schlüsselpaaren.....	24
6.3.1	Archivierung öffentlicher Schlüssel.....	24
6.3.2	Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren .....	24
6.4	Aktivierungsdaten .....	24
6.4.1	Aktivierungsdaten .....	24
6.4.2	Schutz von Aktivierungsdaten .....	24
6.5	Sicherheitsmaßnahmen in den Rechneranlagen .....	24
6.5.1	Spezifische technische Sicherheitsanforderungen in den Rechneranlagen .....	24
6.5.2	Beurteilung von Computersicherheit .....	24
6.6	Technische Maßnahmen während des Life Cycles.....	24
6.6.1	Sicherheitsmaßnahmen bei der Entwicklung .....	24
6.6.2	Sicherheitsmaßnahmen beim Computermanagement.....	24
6.6.3	Sicherheitsmaßnahmen während der Life Cycles.....	24
6.7	Sicherheitsmaßnahmen für Netze .....	24
6.8	Zeitstempel .....	24
<b>7</b>	<b>Profile von Zertifikaten, Sperrlisten und OCSP .....</b>	<b>25</b>
7.1	Zertifikatsprofile .....	25
7.1.1	Versionsnummern .....	25
7.1.2	Zertifikatserweiterungen .....	25
7.1.3	Algorithmen OIDs .....	25
7.1.4	Namensformate .....	25
7.1.5	Namensbeschränkungen.....	25
7.1.6	OIDs der Zertifikatsrichtlinien .....	25
7.1.7	Nutzung der Erweiterung "Policy Constraints" .....	25
7.1.8	Syntax und Semantik von "Policy Qualifiers" .....	25
7.1.9	Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie .....	25
7.2	Sperrlistenprofile .....	25
7.2.1	Versionsnummer(n) .....	25
7.2.2	Erweiterungen von Sperrlisten und Sperrlisteneinträgen .....	25
7.3	Profile des Statusabfragedienstes (OCSP) .....	26
7.3.1	Versionsnummer(n) .....	26
7.3.2	OCSP Erweiterungen .....	26
<b>8</b>	<b>Überprüfungen und andere Bewertungen .....</b>	<b>27</b>
8.1	Häufigkeit und Bedingungen für Überprüfungen .....	27
8.2	Identität/Qualifikation des Prüfers.....	27
8.3	Stellung des Prüfers zum Bewertungsgegenstand .....	27
8.4	Durch Überprüfungen abgedeckte Themen .....	27
8.5	Reaktionen auf Unzulänglichkeiten .....	27
8.6	Information über Bewertungsergebnisse.....	27

<b>9</b>	<b>Andere finanzielle und rechtliche Angelegenheiten .....</b>	<b>28</b>
9.1	Preise.....	28
9.1.1	Preise für Zertifikate oder Zertifikatserneuerungen .....	28
9.1.2	Preise für den Zugriff auf Zertifikate .....	28
9.1.3	Preise für Sperrungen oder Statusinformationen .....	28
9.1.4	Preise für andere Dienstleistungen .....	28
9.1.5	Richtlinien für Rückerstattungen.....	28
9.2	Finanzielle Zuständigkeiten .....	28
9.2.1	Versicherungsdeckung .....	28
9.2.2	Andere Posten .....	28
9.2.3	Versicherung oder Gewährleistung für Endnutzer .....	28
9.3	Vertraulichkeitsgrad von Geschäftsdaten.....	28
9.3.1	Definition von vertraulichen Informationen .....	28
9.3.2	Informationen, die nicht zu den vertraulichen Informationen gehören .....	28
9.3.3	Zuständigkeiten für den Schutz vertraulicher Informationen.....	28
9.4	Datenschutz von Personendaten .....	28
9.4.1	Datenschutzkonzept .....	28
9.4.2	Als persönlich behandelte Daten.....	28
9.4.3	Daten, die nicht als persönlich behandelt werden.....	29
9.4.4	Zuständigkeiten für den Datenschutz.....	29
9.4.5	Hinweis und Einwilligung zur Nutzung persönlicher Daten .....	29
9.4.6	Auskunft gemäß rechtlicher oder staatlicher Vorschriften.....	29
9.4.7	Andere Bedingungen für Auskünfte .....	29
9.5	Geistiges Eigentumsrecht.....	29
9.6	Zusicherungen und Garantien .....	29
9.6.1	Zusicherungen und Garantien der CA.....	29
9.6.2	Zusicherungen und Garantien der RA.....	29
9.6.3	Zusicherungen und Garantien der Zertifikatsnehmer .....	29
9.6.4	Zusicherungen und Garantien der Zertifikatsnutzer .....	29
9.6.5	Zusicherungen und Garantien anderer PKI-Teilnehmer .....	29
9.7	Haftungsausschlüsse.....	29
9.8	Haftungsbeschränkungen.....	29
9.9	Schadensersatz .....	29
9.10	Gültigkeitsdauer und Beendigung .....	29
9.10.1	Gültigkeitsdauer.....	29
9.10.2	Beendigung.....	29
9.10.3	Auswirkung der Beendigung und Weiterbestehen .....	29
9.11	Individuelle Mitteilungen und Absprachen mit Teilnehmern.....	29
9.12	Ergänzungen .....	30
9.12.1	Verfahren für Ergänzungen .....	30
9.12.2	Benachrichtigungsmechanismen und -fristen .....	30
9.12.3	Bedingungen für OID Änderungen .....	30
9.13	Verfahren zur Schlichtung von Streitfällen .....	30
9.14	Zugrunde liegendes Recht .....	30
9.15	Einhaltung geltenden Rechts .....	30
9.16	Sonstige Bestimmungen .....	30
9.16.1	Vollständigkeitserklärung.....	30
9.16.2	Abgrenzungen .....	30
9.16.3	Salvatorische Klausel .....	30
9.16.4	Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht) .....	30
9.16.5	Höhere Gewalt.....	30
9.17	Andere Bestimmungen.....	30
<b>10</b>	<b>Glossar .....</b>	<b>31</b>

## 1 Einleitung

### 1.1 Überblick

Diese Zertifikatsrichtlinie (engl. Certificate Policy CP) ist gerichtet an Teilnehmer der TeleTrusT European Bridge CA (EBCA). Sie enthält Vorgaben und Anforderungen an die teilnehmenden Public-Key-Infrastrukturen (PKIen) sowie an die zum Einsatz kommenden Zertifikate.

In dieser CP sind technische und organisatorische Konformitätsanforderungen formuliert, die zur Schaffung organisationsübergreifender Vertrauensbeziehungen zwischen den Mitgliedern der EBCA dienen. Diese CP folgt der Gliederung des RFC 3647.

Der EBCA Teilnehmer (Teilnehmer) erklärt dass,

- seine CA den Vorgaben und Anforderungen dieser CP entspricht und
- er eine eigene CP (Teilnehmer-CP) erstellt hat, die die Vorgaben dieser CP umsetzt und
- er den Interoperabilitätstest erfolgreich bestanden hat.<sup>1</sup>

Die Publizierung der CA-Zertifikate des Teilnehmers erfolgt in der Zertifikats-Liste der EBCA nach Antragstellung (vgl. 1.5.4) und Vorlage der oben beschriebenen Selbsterklärung.

Diese Certificate Policy beschreibt Sicherheitsanforderungen an den Betrieb von Certification Authorities für die Ausstellung und Nutzung von X.509 konformen Zertifikaten. Darüber hinaus definiert die Richtlinie für Dritte einen Grundschutz für die Nutzung von Zertifikaten. Sie beschreibt damit ein transparentes Sicherheitsniveau für die Vertraulichkeit und Authentisierung von Nachrichten, wie z.B. beim Austausch von E-Mails im S/MIME-Format. Auch für andere Zertifikatszwecke wie die Authentisierung bei SSL/TLS- sind diese Vorgaben innerhalb der EBCA bindend. Bestandsmitgliedern steht ein Übergangszeitraum zur Umsetzung und Dokumentation von einem Jahr ab Verabschiedung der neuen CP zur Verfügung.

Im Fall, dass höhere Sicherheitsanforderungen gelten, erleichtert der Rahmen dieser Richtlinie die individuelle Prüfung der Sicherheitsniveaus der betreffenden PKI.

#### 1.1.1 Ziel dieser Richtlinie

Diese Richtlinie soll die Ziele der EBCA unterstützen. Deren Ziele sind es, mit Hilfe von Public-Key-Infrastrukturen sichere organisationsübergreifende elektronische Geschäftsprozesse zu realisieren.

Es müssen folgende Anforderungen erfüllt sein:

- technische Interoperabilität,
- Vergleichbarkeit der Sicherheitsniveaus
- geeignete Mindeststandards.

Die EBCA bietet eine Plattform für die technische Konformität durch Profilierung der technischen Standards sowie für die Durchführung von Tests zur Feststellung gegenseitiger Interoperabilität.

Mit dieser Richtlinie werden den Mitgliedern der EBCA Vorgaben für Mindeststandards an Sicherheit zum Betrieb einer EBCA konformen PKI gegeben. Der Aufbau nach RFC 3647 ermöglicht eine nach außen transparente und vergleichbare Darstellung der Sicherheitsstandards der innerhalb der EBCA betriebenen PKIen.

Jedes Mitglied der EBCA bestätigt durch die Selbsterklärung, den Anforderungen dieser Richtlinie zu entsprechen. Für die Vergleichbarkeit verfügt jedes Mitglied über eine eigene CP (oder dessen Umsetzung als CPS), die die Mindeststandards dieser CP in geeigneter Weise bestätigen.

Das vorliegende Dokument bzw. seine mitgliederspezifische Ausprägung kann auch als Referenzdokument für vertragliche Regelungen dienen (Eignung als Referenz für bilaterale Verträge).

#### 1.1.2 RFC 3647 Struktur

Das vorliegende Dokument ist nach RFC 3647 aufgebaut und folgt den darin vorgesehenen Gliederungspunkten.

---

<sup>1</sup> Die technische Konformität zur Erreichung von Interoperabilität am Beispiel für sichere E-Mail wird im Dokument "Testspezifikation für den Interoperabilitätstest Interoperabilität und Funktionalität für den Austausch sicherer E-Mails mit Zertifikaten unter der European Bridge CA" (vgl. EBCA S/MIME, siehe 1.6.4 Referenzen) beschrieben.



Der formale Aufbau nach diesem international anerkannten Rahmenwerk verbessert die Transparenz und Vergleichbarkeit gegenüber der bisher üblichen Praxis. Durch diese Struktur soll eine bessere Vergleichbarkeit der Policies und damit der Sicherheitsniveaus erreicht werden.

### 1.1.3 Konventionen

In dieser CP werden (analog zum englischen must/shall – should – may in der Standardisierung) die Begriffe muss – soll – kann verwendet:

- **muss, darf nicht, darf nur**  
Verbindliche Vorgabe der EBCA
- **soll, (sollte)**  
Vorgabe der EBCA, Nichteinhaltung nur in begründeten Ausnahmen
- **kann**  
optional

### **Betrieb nach dem aktuellen Stand der Technik:**

Maßgebend für den Betrieb sind die betriebsinternen Sicherheitsrichtlinien und Standards des Teilnehmers. Dabei können sich diese am aktuellen Stand der IT-Sicherheit orientieren, wie sie z.B. im IT-Grundschutzhandbuch des BSI<sup>2</sup> oder nach ISO/IEC 27001 ff<sup>3</sup> aktuell beschrieben werden.

Ordnungsgemäße Erbringung der Dienstleistung:

Eine ordnungsgemäße Erbringung der Dienstleistung bedeutet, dass sich die Dienstleistung am aktuellen Stand von Technik und organisatorischer Prozesse orientieren kann.

### 1.1.4 Gültigkeit

Diese Richtlinie ist bindend für Mitglieder der EBCA.

## 1.2 Name und Kennzeichnung des Dokuments

Diese Zertifikatsrichtlinie trägt den Titel:

### **Zertifikatsrichtlinie für Mitglieder der European Bridge CA**

Version 2.3 - Datum: 17.07.2014

Der Object Identifier (OID) für dieses Dokument ist: 1.3.6.1.4.1.20351.1.2.1

## 1.3 PKI-Teilnehmer

Teilnehmer sind Organisationen, die eine eigene Public-Key-Infrastruktur betreiben oder einen Trust Service Provider (TSP) beauftragt haben.

### 1.3.1 Zertifizierungsstellen (Certification Authorities)

Certification Authorities (CAs) sind Stellen, die Zertifikate für den Teilnehmer ausstellen und die vertraglichen Verpflichtungen des Teilnehmers der European Bridge CA erfüllen. Teilnehmer-CAs können innerhalb oder außerhalb des Unternehmens/ der Organisation des Teilnehmers liegen.

### 1.3.2 Registrierungsstellen (Registration Authorities)

Registration Authorities (RAs) sind Stellen, die Registrierungen für Zertifikatsnehmer durchführen. Teilnehmer-RAs können innerhalb oder außerhalb des Unternehmens/ der Organisation des Teilnehmers angesiedelt sein.

### 1.3.3 Zertifikatsnehmer

Ein Zertifikatsnehmer soll hier als natürliche Person oder technische Entität verstanden werden, der/die den privaten Schlüssel in seiner alleinigen Verfügungsgewalt verwendet. Sind Zertifikatsnehmer natürliche Personen, so erfolgt die Zuordnung zwischen Zertifikat und Zertifikatsnehmer insofern eindeutig, als ein Signatur- bzw. Authentisierungszertifikat eindeutig auf eine natürliche Identität verweist. Ist ein Zertifikat auf eine Funktion oder Personengruppe ausgestellt, so ist dies im Zertifikatsbetreff (Subject) klar kenntlich zu machen (z.B. durch den Zusatz "Team Certificate", wenn eine Verwechslung mit einem Personenzertifikat nicht anderweitig

---

<sup>2</sup> Bundesamt für Sicherheit der Informationstechnik (BSI), IT-Grundschutzhandbuch, siehe <http://www.bsi.de/gshb>

<sup>3</sup> ISO/IEC 27001 und Folgestandards, <http://www.iso.org>

ausgeschlossen ist). Die verantwortlichen natürlichen oder juristischen Personen haben ein Vertragsverhältnis mit der Teilnehmer-CA über die Ausstellung von Zertifikaten.

#### **1.3.4 Zertifikatsnutzer**

Zertifikatsnutzer sind alle Personen und Organisationen, die Zertifikate von Zertifikatsnehmern nutzen können und Zugang zu den Diensten der EBCA haben.

#### **1.3.5 Andere Teilnehmer**

Teilnehmer, die keine Verpflichtungen gegenüber der EBCA eingegangen sind, sind nicht Bestandteil dieser Richtlinie.

### **1.4 Verwendung von Zertifikaten**

#### **1.4.1 Erlaubte Verwendungen von Zertifikaten**

Der EBCA Teilnehmer muss innerhalb seiner CP die erlaubte Verwendung von Zertifikaten vorgeben.

Maßgeblich für die erlaubte Verwendung von Zertifikaten müssen die im Zertifikat enthaltenen Attribute zur "KeyUsage" sowie die Vorgaben in der zugehörigen CP des Teilnehmers sein.

#### **1.4.2 Verbotene Verwendungen von Zertifikaten**

Keine Vorgaben

### **1.5 Pflege der Richtlinie**

#### **1.5.1 Zuständigkeit für das Dokument**

EBCA Board

TeleTrusT – Bundesverband IT-Sicherheit e.V.  
Chausseestraße 17  
D-10115 Berlin

#### **1.5.2 Ansprechpartner/Kontaktperson/Sekretariat**

TeleTrusT European Bridge CA  
[Serviceverantwortlicher]  
Chausseestraße 17  
D-10115 Berlin

[info@ebca.de](mailto:info@ebca.de)  
<http://www.ebca.de>

Tel.: +49 30 4005 4310  
Fax: +49 30 4005 4311

#### **1.5.3 Pflege dieser Richtlinie**

Diese Richtlinie wird inhaltlich durch die Mitglieder der TeleTrusT-EBCA-AG "Technik" gepflegt. Eine inhaltliche Überprüfung erfolgt anlassbezogen oder alle 3 Jahre und wird durch das Board der EBCA verabschiedet.

Nicht wesentliche Änderungen können durch das folgende Verfahren beschleunigt verabschiedet werden: Die Geschäftsleitung verteilt an die Mitglieder des Boards ein Dokument, in welchem die vorgeschlagenen Änderungen kenntlich gemacht sind und kann eine Frist setzen innerhalb derer Einwände gemacht werden müssen. Gehen innerhalb dieser Frist keine Einwände bei der Geschäftsleitung ein, gilt die neue Version als verabschiedet.

#### **1.5.4 Annahmeverfahren für Teilnehmer-CP<sup>4</sup>**

Der Teilnehmer beantragt die Aufnahme seiner zertifikatsausstellenden CA in die EBCA. Bei externen Zertifikatsdienstleistern wird die Eingrenzung für die Zertifikatssuche über die relevanten Domänen in der E-Mailadresse vorgenommen. Die Beantragung umfasst die Teilnahme am Interoperabilitätstest der EBCA, sowie eine Selbsterklärung. Im Einzelnen erklärt er:

---

<sup>4</sup> Abweichung vom RFC 3647: Der RFC beschreibt wie eine Organisations-CPS aussehen muss. In diesem Dokument wird jedoch eine Bridge-Infrastruktur beschrieben. Aus diesem Grund werden Anforderungen an die CP eines Teilnehmers gestellt.

- dass seine zertifikatsausstellende CA den Anforderungen dieser CP entspricht und
- dass in der angegebenen Teilnehmer-CP die Umsetzung dieser Anforderungen beschrieben ist.

Entspricht die CA des Teilnehmers den Anforderungen nicht in allen Punkten, so beschreibt der EBCA Teilnehmer im Rahmen einer Erklärung zur teilweisen Nicht-Konformität die Stellen, wo keine Entsprechung gegenüber dieser CP vorliegt.

Das Board der EBCA entscheidet, basierend auf den Informationen dieser Selbsterklärung, über die Aufnahme der CA (und damit auch der entsprechenden CPS).

Der Teilnehmer stimmt zu, Änderungen, die nicht mit der bestehenden CP/CPS im Einklang stehen, wie auch die Beendigung seiner Zertifizierungsdienstleistungen, vorher der EBCA anzuzeigen.

Die EBCA ist berechtigt, wenn Teilnehmer die Anforderungen dieser CP nicht erfüllen, die Aufnahme in die EBCA zu verweigern bzw. zu widerrufen.

Das Board kann eine erneute Abgabe der Selbsterklärung verlangen, wenn der Teilnehmer wesentliche Änderungen an seiner PKI und/oder CP vornimmt. Gleiches gilt, wenn die CP der EBCA wesentlich geändert wurde.

### **1.5.5 Zuständiger für die Anerkennung einer CP in Hinblick auf diese CP**

Zuständig für die Anerkennung der CP eines Teilnehmers ist das Board der EBCA.

### **1.6 Begriffe und Abkürzungen**

Begriffe und Abkürzungen finden sich im Anhang.

#### **1.6.1 Deutsche Begriffe**

siehe Glossar.

#### **1.6.2 Englische Begriffe**

siehe Glossar.

#### **1.6.3 Abkürzungen**

siehe Glossar.

#### **1.6.4 Referenzen**

- [RFC 3647], S. Chokhani et. Al., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework",  
Abrufbar unter <http://www.faqs.org/rfcs/rfc3647.html>.
- [EBCA S/MIME], European Bridge CA, "Testspezifikation für den Interoperabilitätstest Interoperabilität und Funktionalität für den Austausch sicherer E-Mails mit Zertifikaten unter der European Bridge CA".
- [ECRYPT], European Network of Excellence in Cryptology (ECRYPT), D.SPA.10 – ECRYPT Yearly Report on Algorithms and Keysizes,  
Abrufbar unter <http://www.ecrypt.eu.org>.
- [ISO 27001], ISO/IEC 27001 - Information security management,  
Abrufbar unter <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>.
- [SigAlg], Bundesnetzagentur, "Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, jährliche Veröffentlichung im Bundesanzeiger.
- [Common PKI] ISIS/MTT Version 1.1, Part 1. Table 12: KeyUsage
- [ITWissen], ITWissen Das große Online-Lexikon für Informationstechnologie,  
Abrufbar unter <http://www.itwissen.info/>.
- [T7], T7 e.V. Berufsverband der Trustcenterbetreiber,  
Abrufbar unter <http://www.t7ev.org/ws/T7-de/Common-PKI>.

## **2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen**

### **2.1 Verzeichnisse**

Der Teilnehmer muss der EBCA und deren Teilnehmern einen Zugriff auf Sperrdaten zur Verfügung stellen. Ein Verzeichnisdienst für den Zugriff auf Zertifikate kann ebenfalls zur Verfügung gestellt werden.

Der Teilnehmer gewährleistet eine ordnungsgemäße Erbringung der Verzeichnis-Dienstleistungen im Rahmen seiner Sicherheitsrichtlinie und orientiert sich am aktuellen Stand der Technik.

Der Teilnehmer muss sicherstellen, dass personenbezogene Daten, die dem Datenschutz unterliegen, nicht ohne Einwilligung der betroffenen Personen über die Kanäle der EBCA publiziert werden.

### **2.2 Veröffentlichung von Informationen zur Zertifikatserstellung**

Der Teilnehmer erklärt sein Einverständnis, die CP oder die den Betrieb der PKI betreffenden Teile seiner Policy sowohl dem Betreiber der EBCA als auch den anderen Teilnehmern zugänglich zu machen.

Der Teilnehmer stimmt einer Veröffentlichung seiner Teilnahme an der EBCA und der Weitergabe seines Root-Zertifikates sowie untergeordneter CA-Zertifikate im Rahmen des EBCA Verbundes zu. **Der Teilnehmer erklärt sich bereit, nach Möglichkeit in seiner CP auf die Teilnahme an der EBCA und das Durchlaufen der Interoperabilitätstests hinzuweisen.**

### **2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen**

Der Teilnehmer muss Zeitpunkt und Häufigkeit der Veröffentlichung von Verzeichnis-Informationen (Sperrinformationen, Verzeichnisdienste) angeben. Die Veröffentlichung von Sperrinformationen muss unverzüglich nach durchgeführter Sperrung des entsprechenden Zertifikates erfolgen.

Die Veröffentlichung der CP des Teilnehmers oder des den Betrieb der PKI betreffenden Teils seiner Policy, Änderungen daran oder deren Architektur, muss (4 Wochen) vorher gegenüber der EBCA erfolgen.

### **2.4 Zugriffskontrollen auf Verzeichnisse**

Der Betreiber der Verzeichnisdienste für Zertifikate und Sperrinformationen gewährleistet eine ordnungsgemäße Zugriffskontrolle, die unkontrollierte Änderungen dieser Informationen verhindert.

### **3 Identifizierung und Authentifizierung**

#### **3.1 Namensregeln**

##### **3.1.1 Arten von Namen**

Die Namensregeln für den "SubjectDistinguishedName" (Subject DN) und "IssuerDistinguishedName" (Issuer DN) müssen nach dem X.501-Standard definiert sein. In Subject DN und Issuer DN muss das Attribut "CommonName" (CN) enthalten sein.

Es wird empfohlen die E-Mail Adresse gesondert in das Feld "SubjectAltName" zu schreiben. Die Namensregeln sollen gemäß RFC 822 erfolgen. E-Mail-Adressen können Teil des DN sein.

##### **3.1.2 Notwendigkeit für aussagefähige Namen**

Zertifikate können sich auf natürliche oder juristische Personen oder technische Entitäten beziehen. Sie müssen jeweils als solche eindeutig kenntlich sein. Sie müssen den Zertifikatsnehmer innerhalb der Gültigkeit der CP eindeutig identifizieren. Zertifikate für organisations- bzw. funktionsbezogene Personengruppen sowie für organisationsbezogene E-Mailstellen müssen sich deutlich von Zertifikaten für natürliche Personen unterscheiden. Eine 1:N-Beziehung bei Zertifikat und Zertifikatsnehmer ist bei End-Entity-Zertifikaten unzulässig. Kenntlich gemachte Gruppenzertifikate bilden eine Ausnahme. Als zusätzliche Maßnahme (z.B. elektronisches Siegel) kann sie dann eingesetzt werden, wenn die eindeutige Identifizierung des Zertifikatsnehmers nicht beeinträchtigt wird.

##### **3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern**

Ein als Pseudonym ausgestelltes Zertifikat muss als solches für Menschen zu erkennen sein. Wenn Zertifikate mit Pseudonymen erstellt werden, muss die Teilnehmer-RA bzw. Teilnehmer-CA die reale Identität des Zertifikatsnehmers in ihren Unterlagen festhalten.

##### **3.1.4 Regeln für die Interpretation verschiedener Namensformen**

Für Zertifikate, die für sichere E-Mail genutzt werden (insbes. Verschlüsselungs- und Authentifizierungszertifikate) muss die E-Mail Adresse des Zertifikatsnehmers eingetragen sein.

##### **3.1.5 Eindeutigkeit von Namen**

Bei der Vergabe von Namen muss sichergestellt sein, dass der gewählte DN innerhalb der ausstellenden CA eindeutig ist. Der Name des CA-Zertifikats muss innerhalb der EBCA eindeutig sein.

##### **3.1.6 Anerkennung, Authentifizierung und Rolle von Markennamen**

Keine Vorgaben.

#### **3.2 Erstmalige Überprüfung der Identität**

##### **3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels**

Keine Vorgaben.

##### **3.2.2 Authentifizierung von Organisationszugehörigkeiten**

Keine Vorgaben.

##### **3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers**

Die Registration Authority gewährleistet eine zuverlässige nach menschlichem Ermessen zweifelsfreie Identifizierung und Prüfung der Antragsdaten im Rahmen der Integritäts-, Authentizitäts- und Vertraulichkeitsanforderungen ihrer Sicherheitsrichtlinie, die sich am aktuellen Stand der Technik orientiert.

##### **3.2.4 Ungeprüfte Zertifikatsnehmerangaben**

Keine Vorgaben.

##### **3.2.5 Prüfung der Berechtigung zur Antragstellung**

Der Prozess für die Prüfung der Berechtigung zur Antragstellung muss dokumentiert werden.

##### **3.2.6 Kriterien zur "Interoperation" (Zusammenwirkung/Wechselwirkung)**

Keine Vorgaben.

### **3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Rekeying)**

#### **3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung**

Keine Vorgaben.

#### **3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen**

Die Registration Authority gewährleistet eine zuverlässige Identifizierung und Prüfung der bisherigen Antragsdaten im Rahmen seiner Sicherheitsrichtlinie.

#### **3.4 Identifizierung und Authentifizierung von Sperranträgen**

Die Registration Authority gewährleistet im Rahmen ihrer Sicherheitsrichtlinie eine zuverlässige Identifizierung und Authentisierung des Antragstellers.

## 4 Betriebsanforderungen

### 4.1 Zertifikatsantrag

#### 4.1.1 Wer kann einen Zertifikatsantrag stellen?

Nur die verantwortliche natürliche oder juristische Person kann Personen-, Organisations- oder Zertifikate für technische Prozesse beantragen. Ein geeignetes Verfahren für den Nachweis der Verantwortung muss dokumentiert sein.

#### 4.1.2 Registrierungsprozess und Zuständigkeiten

Die Registrierung muss ein dokumentierter Prozess sein, der die Anforderungen der Identifizierung nach 3.2.3 erfüllt.

### 4.2 Verarbeitung des Zertifikatsantrags

#### 4.2.1 Durchführung der Identifizierung und Authentifizierung

Vor einer Registrierung sind die Zertifikatsnehmer zuverlässig nach einem dokumentierten Prozess zu identifizieren.

#### 4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Die Vorgaben zur Annahme eines Zertifikatsantrages sind zu dokumentieren. Eine Annahme darf nur für identifizierte Antragsteller erfolgen.

#### 4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgaben.

### 4.3 Zertifikatsausgabe

#### 4.3.1 Aktionen des Zertifizierungsdiensteanbieters (Trust Service Provider) bei der Ausgabe von Zertifikaten

Eine Ausgabe von Zertifikaten darf nur für gültige Zertifikatsanträge erfolgen. Die Aktionen bei der Zertifikatsausgabe müssen anhand dokumentierter Prozesse erfolgen. Dabei muss sichergestellt sein, dass eine eindeutige Verbindung von Zertifikatsnehmer und dem zugehörigen Schlüsselpaar besteht. Die Prüfung erfolgt anhand dokumentierter Prozesse.

#### 4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats durch die CA

Die Benachrichtigung des Zertifikatsnehmers erfolgt anhand entsprechend dokumentierter Prozesse.

### 4.4 Zertifikatsannahme

#### 4.4.1 Verhalten für eine Zertifikatsannahme

Der Prozess für die sichere Zertifikatsübergabe und die Bedingungen, die zu einer Annahme des Zertifikates durch den Teilnehmer führen, müssen dokumentiert werden.

#### 4.4.2 Veröffentlichung des Zertifikats durch die CA

Die CA-Zertifikate der Teilnehmer müssen gegenüber der EBCA veröffentlicht werden.

Neu ausgestellte Endnutzerzertifikate können in einem Verzeichnisdienst veröffentlicht werden.

#### 4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Im Fall der Ausgabe eines CA-Zertifikates, deren CA an der EBCA teilnimmt, muss die EBCA unverzüglich benachrichtigt werden.

Stellt die in der EBCA registrierte CA eines Teilnehmers ein Sub-CA Zertifikat aus, **muss** die EBCA darüber informiert werden und dieses publizieren.

Für Benutzerzertifikate gelten keine Vorgaben.

## **4.5 Verwendung des Schlüsselpaars und des Zertifikats**

### **4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer**

Die Verantwortlichkeiten des Zertifikatsnehmers müssen durch den Trust Service Provider dokumentiert und dem Zertifikatsnehmer mitgeteilt werden.

Der im Zertifikat dokumentierte private Schlüssel des Teilnehmers darf nur für Anwendungen benutzt werden, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen.

Folgende Nutzungsarten sind zulässig:

Authentifizierung von Benutzer- oder Anwendungsdaten und technischen Systemen (Nutzungsart "digital signature")

Entschlüsselung von Benutzer- oder Anwendungsdaten oder von symmetrischen Schlüsseln, welche in dem so genannten Hybridverfahren für die Verschlüsselung solcher Daten dienen (Nutzungsarten "dataEncryption" bzw. "KeyEncryption")

Kennzeichnung der Verbindlichkeit (Nutzungsart "non-repudiation"/"content-commitment") einer elektronischen Signatur durch den Zertifikatsnehmer.

### **4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer**

Keine Vorgaben.

## **4.6 Zertifikatserneuerung**

### **4.6.1 Bedingungen für eine Zertifikatserneuerung**

Eine Zertifikatserneuerung unter Beibehaltung des asymmetrischen Schlüsselpaars darf nur dann erfolgen, wenn die bisher eindeutige Verbindung von Zertifikatsnehmer und privaten Schlüssel sicher gestellt bleibt.

Die Bedingungen für eine Zertifikatserneuerung müssen dokumentiert werden.

### **4.6.2 Wer darf eine Zertifikatserneuerung beantragen?**

Die CA dokumentiert, wie die Berechtigung geprüft wird.

### **4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung**

Die Bearbeitung eines Antrags auf Zertifikatserneuerung muss ein dokumentierter Prozess sein, der die Anforderungen der Identifizierung nach 3.2.3 erfüllt.

### **4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats**

Die Benachrichtigung des Zertifikatsnehmers erfolgt entsprechend dokumentierter Prozesse.

### **4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung**

Der Prozess für die sichere Zertifikatsübergabe und Bedingungen, die zu einer Annahme des Zertifikates durch den Teilnehmer führen, müssen dokumentiert werden.

### **4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA**

Ein erneuertes CA-Zertifikat muss gegenüber der EBCA unverzüglich veröffentlicht werden.

Erneuerte Endnutzertifikate können in einem Verzeichnisdienst veröffentlicht werden.

### **4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats**

Die Erneuerung eines CA-Zertifikates muss gegenüber der EBCA unverzüglich angezeigt werden.

Für Benutzerzertifikate gelten keine Vorgaben.

## **4.7 Zertifizierung nach Schlüsselerneuerung**

### **4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung**

Die Certification Authority muss Bedingungen beschreiben, unter welchen Umständen ein neu erzeugtes Schlüsselpaar zusammen mit den bisherigen Zertifikatsdaten zertifiziert wird. Bedingungen sind zum Beispiel:

- Sperrung des bisherigen Zertifikats aufgrund einer Schlüsselkompromittierung,
- Ablauf des bestehenden Zertifikates,



#### **4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?**

Die CA dokumentiert, wie die Berechtigung geprüft wird.

#### **4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen**

Keine Vorgaben.

#### **4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats**

Die Benachrichtigung des Zertifikatsnehmers erfolgt entsprechend dokumentierter Prozesse.

#### **4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen**

Der Prozess für die sichere Zertifikatsübergabe und Bedingungen, die zu einer Annahme des Zertifikates durch den Teilnehmer führen, müssen dokumentiert werden.

#### **4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA**

Ein erneuertes CA-Zertifikat muss gegenüber der EBCA unverzüglich veröffentlicht werden.  
Neu ausgestellte Endnutzerzertifikate können in einem Verzeichnisdienst veröffentlicht werden.

#### **4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats**

Die Erneuerung eines CA-Zertifikates muss gegenüber der EBCA unverzüglich angezeigt werden.  
Für Benutzerzertifikate gelten keine Vorgaben.

### **4.8 Zertifikatsänderung**

#### **4.8.1 Bedingungen für eine Zertifikatsänderung**

Die Certification Authority muss Bedingungen beschreiben, unter welchen Umständen eine Zertifikatsänderung durchgeführt wird. Bedingungen sind zum Beispiel:

- der Name im Zertifikat erlaubt keine eindeutige Zuordnung zum Zertifikatsnehmer,
- die Zuordnung der im Zertifikat enthaltenen E-Mail-Adresse zum Zertifikatsnehmer ist nicht mehr gegeben.

Technisch bedeutet dies eine Neuzertifizierung.

#### **4.8.2 Wer darf eine Zertifikatsänderung beantragen?**

Die CA dokumentiert, wie die Berechtigung geprüft wird.

#### **4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung**

Keine Vorgaben.

#### **4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats**

Die Benachrichtigung des Zertifikatsnehmers erfolgt entsprechend dokumentierter Prozesse.

#### **4.8.5 Verhalten für die Annahme einer Zertifikatsänderung**

Der Prozess für die sichere Zertifikatsübergabe und Bedingungen, die zu einer Annahme des Zertifikates durch den Teilnehmer führen, müssen dokumentiert werden.

#### **4.8.6 Veröffentlichung der Zertifikatsänderung durch die CA**

Ein geändertes CA-Zertifikat muss gegenüber der EBCA unverzüglich veröffentlicht werden.  
Neu ausgestellte Endnutzerzertifikate können in einem Verzeichnisdienst veröffentlicht werden.

#### **4.8.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines neuen Zertifikats**

Die Änderung eines CA-Zertifikates muss gegenüber der EBCA unverzüglich angezeigt werden.  
Für Benutzerzertifikate gelten keine Vorgaben.

### **4.9 Sperrung und Suspendierung von Zertifikaten**

#### **4.9.1 Bedingungen für eine Sperrung**

Die Certification Authority muss Bedingungen beschreiben, unter welchen Umständen eine Zertifikatssperrung durchgeführt wird. Eine Sperrung muss erfolgen wenn:

- eine Kompromittierung des Schlüssels vorliegt,
- die eindeutige Zuordnung des Schlüsselpaars zu seinem Zertifikatsnehmer nicht mehr gegeben ist,
- die eindeutige Verbindung zwischen Zertifikat und Schlüssel nicht mehr gegeben ist.

Eine Kompromittierung des privaten Signaturschlüssels der Certification Authority (CA) ist der EBCA unverzüglich anzuzeigen.

#### **4.9.2 Wer kann eine Sperrung beantragen?**

Die CA dokumentiert, wie die Berechtigung geprüft wird.

#### **4.9.3 Verfahren für einen Sperrantrag**

Sowohl die Registration Authority, als auch die Certification Authority müssen das Verfahren für die Sperrung eines Zertifikates dokumentieren.

#### **4.9.4 Fristen für einen Sperrantrag**

Die Certification Authority soll Fristen für einen Sperrantrag gegenüber dem Zertifikatsnehmer dokumentieren.

#### **4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch den Zertifizierungsdiensteanbieter (Trust Service Provider)**

Eine Zertifikatssperrung muss unverzüglich erfolgen.

#### **4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen**

Die verfügbaren Methoden zum Prüfen von Sperrinformationen müssen den Konformitätskriterien der EBCA entsprechen.

#### **4.9.7 Frequenz der Veröffentlichung von Sperrlisten**

Die Frequenz der Veröffentlichung von Sperrlisten muss von der Certification Authority dokumentiert werden. Dabei soll eine zeitnahe Verfügbarkeit von aktuellen Sperrinformationen gewährleistet sein.

#### **4.9.8 Maximale Latenzzeit für Sperrlisten**

Die maximale Latenzzeit für Sperrlisten muss von der Certification Authority dokumentiert sein.

#### **4.9.9 Verfügbarkeit von Online-Sperrinformationen**

Sperrinformationen müssen online zur Verfügung stehen.

#### **4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen**

In den im Zertifikat anzugebenden CRL-Verteilungspunkten (CDP) **muss** mindestens eine öffentlich zugängliche http- oder LDAP-Adresse angegeben sein, die eine Online-Prüfung des Zertifikats ermöglicht. Es **sollte** sowohl eine http- als auch LDAP-Abfrage möglich sein. Eine OCSP-Abfrage kann zusätzlich möglich sein.

#### **4.9.11 Andere Formen zur Anzeige von Sperrinformationen**

Sperrinformationen müssen online zur Verfügung gestellt werden. Die Verfügbarkeit dieser Online-Dienstleistung muss dokumentiert werden.

#### **4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels**

Keine Vorgaben.

#### **4.9.13 Bedingungen für eine Suspendierung**

Dieser Status muss online angezeigt werden.

#### **4.9.14 Wer kann eine Suspendierung beantragen?**

Keine Vorgaben.

#### **4.9.15 Verfahren für Anträge auf Suspendierung**

Keine Vorgaben.

#### **4.9.16 Begrenzungen für die Dauer von Suspendierungen**

Keine Vorgaben.

#### **4.10 Statusabfragedienst für Zertifikate**

##### **4.10.1 Funktionsweise des Statusabfragedienstes**

Bei Betrieb eines Online-Statusabfragedienstes muss die Funktionsweise beschrieben sein.

##### **4.10.2 Verfügbarkeit des Statusabfragedienstes**

Die Verfügbarkeit des Statusabfragedienstes muss dokumentiert werden. Dabei soll eine zeitnahe Verfügbarkeit von aktuellen Statusinformationen gewährleistet sein.

##### **4.10.3 Optionale Leistungen**

Keine Vorgaben.

#### **4.11 Kündigung durch den Zertifikatsnehmer**

Im Fall einer Kündigung durch den Zertifikatsnehmer muss das Zertifikat gesperrt werden.

#### **4.12 Schlüssel hinterlegung und Wiederherstellung**

##### **4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel**

Im Fall einer Schlüssel hinterlegung muss der Trust Service Provider die Prozesse der Schlüssel hinterlegung dokumentieren. Diese müssen der eigenen Sicherheitsrichtlinie und dem aktuellen Stand der Technik entsprechen. Eine Schlüssel hinterlegung soll nicht für Signaturschlüssel erfolgen.

##### **4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln**

Keine Vorgaben.

## 5 Nicht-technische Sicherheitsmaßnahmen

Nicht-technische Sicherheitsmaßnahmen erfolgen anhand dokumentierter Prozesse und Vorgaben, die Teil der Sicherheitsrichtlinie des Teilnehmers sind und sich am aktuellen Stand der Technik orientieren sollen. Diese Sicherheitsmaßnahmen werden vom Teilnehmer ordnungsgemäß erbracht, um die in Kapitel 4 beschriebenen Betriebsanforderungen zu erfüllen.

Um die Struktur des RFC 3647 beizubehalten, sind in diesem Dokument die Überschriften angegeben.

Im CP des Teilnehmers müssen zumindest die Anforderungen zu nachfolgenden Abschnitten publiziert werden:

- Abschnitt 5.6 Schlüsselwechsel beim Zertifizierungsdiensteanbieter (Trust Service Provider)
- Abschnitt 5.7 Kompromittierung des privaten Schlüssels des Zertifizierungsdiensteanbieters (Trust Service Provider)
- Abschnitt 5.8 Schließung eines Zertifizierungsdiensteanbieters (Trust Service Providers) oder einer Registrierungsstelle (Registration Authority)

### 5.1 Bauliche Sicherheitsmaßnahmen

#### 5.1.1 Lage und Gebäude

Die PKI muss in Europa (EU + EFTA) betrieben werden. Abweichungen bei Teilnehmern, die die PKI von einem professionellen Trustcenter betreiben lassen, sind möglich und erfordern eine Zustimmung des EBCA-Lenkungsgremiums. Bezugspunkt für eine Entscheidung ist der Betriebsstandort für die EBCA-relevante Root- bzw. Sub-CA.

#### 5.1.2 Zugang

Keine Vorgaben.

#### 5.1.3 Strom, Heizung und Klimaanlage

Keine Vorgaben.

#### 5.1.4 Wassergefährdung

Keine Vorgaben.

#### 5.1.5 Brandschutz

Keine Vorgaben.

#### 5.1.6 Lager und Archiv

Keine Vorgaben.

#### 5.1.7 Müllbeseitigung

Keine Vorgaben.

#### 5.1.8 Desaster Backup

Keine Vorgaben.

### 5.2 Verfahrensvorschriften

#### 5.2.1 Rollenkonzept

Keine Vorgaben.

#### 5.2.2 Mehraugenprinzip

Keine Vorgaben.

#### 5.2.3 Rollenausschlüsse

Keine Vorgaben.

#### 5.2.4 Rollentrennung

Keine Vorgaben.

### **5.3 Personalkontrolle**

#### **5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit**

Keine Vorgaben.

#### **5.3.2 Methoden zur Überprüfung der Rahmenbedingungen**

Keine Vorgaben.

#### **5.3.3 Anforderungen an Schulungen**

Keine Vorgaben.

#### **5.3.4 Häufigkeit von Schulungen und Belehrungen**

Keine Vorgaben.

#### **5.3.5 Häufigkeit und Folge von Job-Rotation**

Keine Vorgaben.

#### **5.3.6 Maßnahmen bei unerlaubten Handlungen**

Keine Vorgaben.

#### **5.3.7 Anforderungen an freie Mitarbeiter**

Keine Vorgaben.

#### **5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen**

Keine Vorgaben.

### **5.4 Überwachungsmaßnahmen**

#### **5.4.1 Arten von aufgezeichneten Ereignissen**

Keine Vorgaben.

#### **5.4.2 Häufigkeit der Bearbeitung der Aufzeichnungen**

Keine Vorgaben.

#### **5.4.3 Aufbewahrungszeit von Aufzeichnungen**

Keine Vorgaben.

#### **5.4.4 Sicherung der Aufzeichnungen**

Keine Vorgaben.

#### **5.4.5 Datensicherung der Aufzeichnungen**

Keine Vorgaben.

#### **5.4.6 Speicherung der Aufzeichnungen (intern/extern)**

Keine Vorgaben.

#### **5.4.7 Benachrichtigung der Ereignisauslöser**

Keine Vorgaben.

#### **5.4.8 Verwundbarkeitsabschätzungen**

Keine Vorgaben.

### **5.5 Archivierung von Aufzeichnungen**

#### **5.5.1 Arten von archivierten Aufzeichnungen**

Keine Vorgaben.

#### **5.5.2 Aufbewahrungsfristen für archivierte Daten**

Keine Vorgaben.

### **5.5.3 Sicherung des Archivs**

Keine Vorgaben.

### **5.5.4 Datensicherung des Archivs**

Keine Vorgaben.

### **5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen**

Keine Vorgaben.

### **5.5.6 Archivierung (intern/extern)**

Keine Vorgaben.

### **5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen**

Keine Vorgaben.

## **5.6 Schlüsselwechsel beim Zertifizierungsdiensteanbieter (Trust Service Provider)**

Im Regelwerk des EBCA-Teilnehmers werden in diesem Kapitel punktuell Angaben erwartet.

## **5.7 Kompromittierung und Geschäftsweiterführung beim Zertifizierungsdiensteanbieter (Trust Service Provider)**

Im Regelwerk des EBCA-Teilnehmers werden in diesem Kapitel punktuell Angaben erwartet.

### **5.7.1 Behandlung von Vorfällen und Kompromittierungen**

Siehe 5.7.

### **5.7.2 Rechnerressourcen-, Software- und/oder Datenkompromittierung**

Siehe 5.7.

### **5.7.3 Verhalten bei Kompromittierung des privaten Schlüssels des Zertifizierungsdiensteanbieters (Trust Service Providers)**

Siehe 5.7.

### **5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung**

Siehe 5.7.

## **5.8 Schließung eines Zertifizierungsdiensteanbieters (Trust Service Providers) oder einer Registrierungsstelle (Registration Authority)**

Im Regelwerk des EBCA-Teilnehmers werden in diesem Kapitel punktuell Angaben erwartet.

## 6 Technische Sicherheitsmaßnahmen

Technische Sicherheitsmaßnahmen erfolgen anhand dokumentierter Prozesse und Vorgaben, die sich am aktuellen Stand der Technik orientieren. Diese Sicherheitsmaßnahmen werden vom Teilnehmer ordnungsgemäß erbracht, um die in Kapitel 4. beschriebenen Anforderungen zu erfüllen.

Die verwendeten kryptographischen Verfahren und Protokolle müssen dem aktuellen Stand der Sicherheitsbetrachtungen kryptographischer Verfahren und den jeweils gültigen gesetzlichen Vorgaben entsprechen.

Um die Struktur des RFC 3647 beizubehalten, sind in diesem Dokument die Überschriften angegeben.

Im CP des Teilnehmers müssen zumindest die Anforderungen zu nachfolgenden Abschnitten publiziert werden:

- Abschnitt 6.1 Erzeugung und Installation von Schlüsselpaaren
- Abschnitt 6.2.4 Sicherung privater Schlüssel
- Abschnitt 6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

### 6.1 Erzeugung und Installation von Schlüsselpaaren

Im Regelwerk des EBCA-Teilnehmers werden in diesem Kapitel punktuell Angaben erwartet.

#### 6.1.1 Erzeugung von Schlüsselpaaren

Siehe 6.1.

#### 6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Siehe 6.1.

#### 6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Siehe 6.1.

#### 6.1.4 Lieferung öffentlicher Schlüssel des Zertifizierungsdiensteanbieters (Trust Service Provider) an Zertifikatsnutzer

Siehe 6.1.

#### 6.1.5 Schlüssellängen

Die verwendeten Schlüssellängen sollten sich am aktuellen Stand der Technik orientieren [ECRYPT, Algorithmen-Katalog der Bundesnetzagentur, wie im Bundesanzeiger jeweils jahresaktuell veröffentlicht].

#### 6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Keine Vorgaben.

#### 6.1.7 Schlüsselverwendungen

Keine Vorgaben.

### 6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

Keine Vorgaben, siehe 6.2.4.

#### 6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Keine Vorgaben.

#### 6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

Keine Vorgaben.

#### 6.2.3 Hinterlegung privater Schlüssel

Keine Vorgaben.

#### 6.2.4 Sicherung privater Schlüssel

Im Regelwerk des EBCA-Teilnehmers werden in diesem Kapitel punktuell Angaben erwartet.

#### 6.2.5 Archivierung privater Schlüssel

Siehe 6.2.4.

### **6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen**

Siehe 6.2.4.

### **6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen**

Siehe 6.2.4.

### **6.2.8 Aktivierung privater Schlüssel**

Siehe 6.2.4.

### **6.2.9 Deaktivierung privater Schlüssel**

Siehe 6.2.4.

### **6.2.10 Zerstörung privater Schlüssel**

Siehe 6.2.4.

### **6.2.11 Beurteilung kryptographischer Module**

Siehe 6.2.4.

## **6.3 Andere Aspekte des Managements von Schlüsselpaaren**

### **6.3.1 Archivierung öffentlicher Schlüssel**

Keine Vorgaben.

### **6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren**

Im Regelwerk des EBCA-Teilnehmers werden in diesem Kapitel punktuell Angaben erwartet.

## **6.4 Aktivierungsdaten**

### **6.4.1 Aktivierungsdaten**

Keine Vorgaben.

### **6.4.2 Schutz von Aktivierungsdaten**

Keine Vorgaben.

## **6.5 Sicherheitsmaßnahmen in den Rechneranlagen**

### **6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen**

Keine Vorgaben.

### **6.5.2 Beurteilung von Computersicherheit**

Keine Vorgaben.

## **6.6 Technische Maßnahmen während des Life Cycles**

### **6.6.1 Sicherheitsmaßnahmen bei der Entwicklung**

Keine Vorgaben.

### **6.6.2 Sicherheitsmaßnahmen beim Computermanagement**

Keine Vorgaben.

### **6.6.3 Sicherheitsmaßnahmen während der Life Cycles**

Keine Vorgaben.

## **6.7 Sicherheitsmaßnahmen für Netze**

Keine Vorgaben.

## **6.8 Zeitstempel**

Keine Vorgaben.



## **7 Profile von Zertifikaten, Sperrlisten und OCSP**

### **7.1 Zertifikatsprofile**

#### **7.1.1 Versionsnummern**

Zertifikate müssen konform zum Standard X.509 v3 (Typ 0x2) sein.

#### **7.1.2 Zertifikatserweiterungen**

Die Certification Authority muss die Zertifikatserweiterungen definieren. Dabei sollen Konformitätskriterien der EBCA berücksichtigt werden. Grundsätzlich wird empfohlen, möglichst wenige Zertifikatserweiterungen auf kritisch ("critical") zu setzen.

Folgende Zertifikatserweiterungen müssen kritisch sein:

- "KeyUsage",
- "BasicConstraints" (nur obligatorisch, wenn es sich um ein CA-Zertifikat handelt).

Für die "KeyUsage" und "BasicConstraints" (von CA Zertifikaten) müssen die Vorgaben der Common PKI eingehalten werden (vgl. Common PKI, siehe Referenzen 1.6.4).

Zertifikate, die für sichere E-Mail genutzt werden, müssen die E-Mail-Adresse des Zertifikatshalters enthalten, entweder

- Im "SubjectAltName" (RFC 822Name, bevorzugt) oder
- Innerhalb des "DistinguishedName" (DN)
- In technischen Zertifikaten sollte der primäre Systemname im "Distinguished Name" (DN) aufgenommen werden.

#### **7.1.3 Algorithmen OIDs**

Keine Vorgaben.

#### **7.1.4 Namensformate**

Die CA muss Namensformate dokumentieren. Grundsätzlich sollen Konformitätskriterien der EBCA beachtet werden. Darüber hinaus gelten die folgenden Anforderungen.

Im "DistinguishedName" (DN) muss der "CommonName" (CN) angegeben werden.

#### **7.1.5 Namensbeschränkungen**

Keine Vorgaben.

#### **7.1.6 OIDs der Zertifikatsrichtlinien**

Es wird empfohlen, der OID dieser CP als nicht kritische Erweiterung in das Attribut "certificatePolicies" einzutragen.

#### **7.1.7 Nutzung der Erweiterung "Policy Constraints"**

Keine Vorgaben.

#### **7.1.8 Syntax und Semantik von "Policy Qualifiers"**

Keine Vorgaben.

#### **7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie**

Keine Vorgaben.

### **7.2 Sperrlistenprofile**

#### **7.2.1 Versionsnummer(n)**

Es müssen Sperrlisten der Version 1 (Typ 0x0) oder höher verwendet werden. Im Sinne der Interoperabilität sollten jedoch Sperrlisten mit Version 2 (Typ 0x1) eingesetzt werden.

#### **7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen**

Keine Vorgaben.

### **7.3 Profile des Statusabfragedienstes (OCSP)**

#### **7.3.1 Versionsnummer(n)**

Aktuell: Einsatz von OCSPv1, künftig: Verwendung von SCVP

#### **7.3.2 OCSP Erweiterungen**

Stellt die Certification Authority eine OCSP-Statusprüfung zur Verfügung, muss diese Erweiterung dokumentiert werden. Für die Definition dieser Erweiterungen sollen Konformitätskriterien der EBCA berücksichtigt werden.

## **8 Überprüfungen und andere Bewertungen**

Überprüfungen und andere Bewertungen der Teilnehmer PKIs erfolgen anhand dokumentierter Prozesse und Vorgaben, die Teil der Sicherheitsrichtlinie des Teilnehmers sind und sich am aktuellen Stand der Technik orientieren. Überprüfungen werden vom Teilnehmer ordnungsgemäß erbracht.

Um die Struktur des RFC 3647 beizubehalten, sind in diesem Dokument die Überschriften angegeben ohne Vorgaben zur inhaltlichen Ausgestaltung zu machen.

### **8.1 Häufigkeit und Bedingungen für Überprüfungen**

Keine Vorgaben.

### **8.2 Identität/Qualifikation des Prüfers**

Keine Vorgaben.

### **8.3 Stellung des Prüfers zum Bewertungsgegenstand**

Keine Vorgaben.

### **8.4 Durch Überprüfungen abgedeckte Themen**

Keine Vorgaben.

### **8.5 Reaktionen auf Unzulänglichkeiten**

Keine Vorgaben.

### **8.6 Information über Bewertungsergebnisse**

Keine Vorgaben.

## **9 Andere finanzielle und rechtliche Angelegenheiten**

Teil der CP des Teilnehmers sind finanzielle und rechtliche Angelegenheiten, die sich an das geltende Recht halten müssen.

Um die Struktur des RFC 3647 beizubehalten, sind in diesem Dokument die Überschriften angegeben ohne Vorgaben zur inhaltlichen Ausgestaltung zu machen.

Im CP des Teilnehmers sollten zumindest die Anforderungen zu nachfolgenden Abschnitten publiziert werden:

- Abschnitt 9.4 Datenschutz von Personendaten
- Abschnitt 9.10 Gültigkeitsdauer und Beendigung
- Abschnitt 9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern
- Abschnitt 9.14 Zugrunde liegendes Recht

### **9.1 Preise**

#### **9.1.1 Preise für Zertifikate oder Zertifikatserneuerungen**

Keine Vorgaben.

#### **9.1.2 Preise für den Zugriff auf Zertifikate**

Keine Vorgaben.

#### **9.1.3 Preise für Sperrungen oder Statusinformationen**

Keine Vorgaben.

#### **9.1.4 Preise für andere Dienstleistungen**

Keine Vorgaben.

#### **9.1.5 Richtlinien für Rückerstattungen**

Keine Vorgaben.

### **9.2 Finanzielle Zuständigkeiten**

#### **9.2.1 Versicherungsdeckung**

Keine Vorgaben.

#### **9.2.2 Andere Posten**

Keine Vorgaben.

#### **9.2.3 Versicherung oder Gewährleistung für Endnutzer**

Keine Vorgaben.

### **9.3 Vertraulichkeitsgrad von Geschäftsdaten**

#### **9.3.1 Definition von vertraulichen Informationen**

Keine Vorgaben.

#### **9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören**

Keine Vorgaben.

#### **9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen**

Keine Vorgaben.

### **9.4 Datenschutz von Personendaten**

Die deutsche Datenschutzgesetzgebung sollte, wenn möglich, als Orientierung verwendet werden.

#### **9.4.1 Datenschutzkonzept**

Keine Vorgaben.

#### **9.4.2 Als persönlich behandelte Daten**

Keine Vorgaben.

**9.4.3 Daten, die nicht als persönlich behandelt werden**

Keine Vorgaben.

**9.4.4 Zuständigkeiten für den Datenschutz**

Keine Vorgaben.

**9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten**

Keine Vorgaben.

**9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften**

Keine Vorgaben.

**9.4.7 Andere Bedingungen für Auskünfte**

Keine Vorgaben.

**9.5 Geistiges Eigentumsrecht**

Keine Vorgaben.

**9.6 Zusicherungen und Garantien**

**9.6.1 Zusicherungen und Garantien der CA**

Keine Vorgaben.

**9.6.2 Zusicherungen und Garantien der RA**

Keine Vorgaben.

**9.6.3 Zusicherungen und Garantien der Zertifikatsnehmer**

Keine Vorgaben.

**9.6.4 Zusicherungen und Garantien der Zertifikatsnutzer**

Keine Vorgaben.

**9.6.5 Zusicherungen und Garantien anderer PKI-Teilnehmer**

Keine Vorgaben.

**9.7 Haftungsausschlüsse**

Keine Vorgaben.

**9.8 Haftungsbeschränkungen**

Keine Vorgaben.

**9.9 Schadensersatz**

Keine Vorgaben.

**9.10 Gültigkeitsdauer und Beendigung**

Keine Vorgaben.

**9.10.1 Gültigkeitsdauer**

Keine Vorgaben.

**9.10.2 Beendigung**

Keine Vorgaben.

**9.10.3 Auswirkung der Beendigung und Weiterbestehen**

Keine Vorgaben.

**9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern**

Keine Vorgaben.

## **9.12 Ergänzungen**

### **9.12.1 Verfahren für Ergänzungen**

Keine Vorgaben.

### **9.12.2 Benachrichtigungsmechanismen und -fristen**

Keine Vorgaben.

### **9.12.3 Bedingungen für OID Änderungen**

Keine Vorgaben.

## **9.13 Verfahren zur Schlichtung von Streitfällen**

Keine Vorgaben.

## **9.14 Zugrunde liegendes Recht**

Keine Vorgaben.

## **9.15 Einhaltung geltenden Rechts**

Keine Vorgaben.

## **9.16 Sonstige Bestimmungen**

### **9.16.1 Vollständigkeitserklärung**

Keine Vorgaben.

### **9.16.2 Abgrenzungen**

Keine Vorgaben.

### **9.16.3 Salvatorische Klausel**

Keine Vorgaben.

### **9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)**

Keine Vorgaben.

### **9.16.5 Höhere Gewalt**

Keine Vorgaben.

## **9.17 Andere Bestimmungen**

## 10 Glossar

<b>Certification Authority</b>	Eine Certification Authority (CA) ist "für das Erstellen, die Ausgabe, Verwaltung und Sperrung von digitalen Zertifikaten zuständig" (vgl. ITWissen, siehe 1.6.4. Referenzen). Im Rahmen der European Bridge CA müssen teilnehmende CAs dabei die vertraglichen Verpflichtungen der European Bridge CA erfüllen. Teilnehmer CAs können dabei innerhalb oder außerhalb der Organisation des Teilnehmers liegen.
<b>Certificate Policy der EBCA</b>	Das Dokument beschreibt Anforderungen für Teilnehmer der EBCA. Der Teilnehmer bestätigt die Einhaltung der EBCA-CP-Vorgaben in seinem CP oder auch Certification Practice Statement (CPS). Die CP der EBCA ist dabei konform zum RFC 3647. Dies wird auch von den CPs der EBCA-Teilnehmer erwartet. Werden für die Zertifikatsbeschaffung (Registrierung, Zertifizierung, Veröffentlichung etc.) Trust Service Provider mit eigener CP in Anspruch genommen, so hat der EBCA-Teilnehmer trotzdem zu den Regelungspflichten, die in seinem Verantwortungsbereich liegen (in Bezug auf den Umgang mit Schlüsselmaterial, im Vorgehen beim Sperren von Zertifikaten, etc.), Stellung zu nehmen.
<b>Certification Practice Statement</b>	Bei dem Certification Practice Statement (CPS) handelt es sich um ein Dokument in dem die Arbeitsweise einer PKI im Allgemeinen detaillierter als im CP beschrieben ist. Ein CPS konkretisiert die in der CP (Certificate Policy) veröffentlichten Sicherheitsvorgaben der PKI und regelt den praktischen Betrieb. Während jedes EBCA-Mitglied für die Vergleichbarkeit über eine eigene CP verfügen muss ist die Veröffentlichung einer CPS nicht notwendig, wenn die Mindeststandards in der CP in geeigneter Weise bestätigt werden.
<b>Certificate Revocation List</b>	Certificate Revocation List (CRL) ist eine Sperrliste, die Informationen über gesperrte Zertifikate enthält um deren Missbrauch zu verhindern. Die Sperrliste umfasst die aktuellen Seriennummern der ungültigen Zertifikate. Sie werden von der Certification Authority (CA) erstellt und signiert und zum Download bereitgestellt. Zur Überprüfung der Gültigkeit von Zertifikaten können auch LDAP- Verzeichnisdienste oder eine Statusanfrage an einen OCSP-Server verwendet werden.
<b>Certificate Revocation</b>	Um den Missbrauch von digitalen Zertifikaten zu verhindern, können oder müssen diese in bestimmten Fällen gesperrt und widerrufen werden, bevor ihre Gültigkeit abläuft. Durch einen Widerruf wird der Gebrauch eines Zertifikats und der zugehörigen PSE dauerhaft unterbunden; denn eine nachfolgende Aufhebung eines Widerrufs ist im Rahmen der Vorgaben des EBCA-CPs nicht erlaubt. Eine Sperrung muss erfolgen, wenn eine Kompromittierung des privaten Schlüssels vorliegt, die eindeutige Zuordnung des Schlüsselpaars zu seinem Zertifikatsnehmer nicht mehr gegeben ist oder die eindeutige Verbindung zwischen Zertifikat und Schlüssel nicht mehr gegeben ist. Eine Kompromittierung des privaten Signaturschlüssels einer Certification Authority (CA) ist der EBCA durch das EBCA-Mitglied unverzüglich anzuzeigen. Die EBCA-Teilnehmer müssen zur Prüfung von Sperrinformationen mindestens eine öffentlich zugängliche http- oder LDAP-Adresse bereitstellen, welche in den CRL-Verteilungspunkten (CDP) der Zertifikate anzugeben sind.
<b>Common PKI</b>	"Die Common PKI Spezifikation beschreibt ein Profil über international verbreitete und anerkannte Standards für elektronische Signaturen, Verschlüsselung und Public-Key-Infrastrukturen" (vgl. T7, siehe 1.6.4. Referenzen). Die Common PKI Spezifikationen stellen die Standards dar, auf welche sich die EBCA-Teilnehmer beim Interoperabilitätstest verständigt haben.
<b>Certificate Distribution Point</b>	Ein Certificate Distribution Point (CDP bzw. auch CRLDP) ist ein im Zertifikat angegebener Sperrlistenverteilpunkt, an dem die Sperrliste (CRL) hinterlegt ist.

<b>DistinguishedName</b>	"DistinguishedName" (DN) ist ein aus mehreren Namensbestandteilen bestehender technischer Name, der in Zertifikaten die ausstellende CA und/oder den Zertifikatnehmer innerhalb der Zertifikatspfade eindeutig beschreibt. "Der DN-Name stellt sicher, dass nie ein digitales Zertifikat für verschiedene Personen mit dem gleichen Namen ausgestellt wird" (vgl. ITWissen, siehe 1.6.4. Referenzen). Für die Eindeutigkeit eines digitalen Zertifikats sind neben dem Namen die Certification Authority und die Seriennummer hinterlegt. Der "DistinguishedName" ist im Standard X.501 definiert. Im Rahmen der EBCA muss bei Zertifikaten die E-Mail-Adresse des Zertifikatsnehmers im "DistinguishedName" (DN) enthalten sein. Weiterhin muss im "DistinguishedName" (DN) der "CommonName" (CN) angegeben werden.
<b>End-Entity-Zertifikate</b>	End-Entity-Zertifikate sind Zertifikate, die direkt auf eine natürliche Person oder technische (End-) Entität ausgestellt sind. Sind Zertifikatsnehmer natürliche Personen, so erfolgt bei der EBCA die Zuordnung zwischen Zertifikat und Zertifikatsnehmer insofern eindeutig, als ein Signatur- bzw. Authentisierungszertifikat eindeutig auf eine natürliche Identität verweist. Ist ein Zertifikat auf eine Funktion oder Personengruppe ausgestellt, so ist dies im Zertifikatsbetreff ("Subject") klar kenntlich zu machen (z.B. durch den Zusatz "Team Certificate", wenn eine Verwechslung mit einem Personenzertifikat nicht anderweitig ausgeschlossen ist).
<b>European Bridge CA</b>	Die TeleTrusT European Bridge CA (EBCA) ist ein Zusammenschluss einzelner, gleichberechtigter Public-Key-Infrastrukturen (PKIen) zu einem PKI-Verbund. Sie ermöglicht eine sichere und authentische Kommunikation zwischen den beteiligten Unternehmen, Institutionen und öffentlichen Verwaltungen.
<b>ISO/IEC 27001</b>	ISO/IEC 27001 ist der Standard für Informationssicherheitsmanagement (ISM) der Internationalen Organisation für Standardisierung (ISO), welcher zum Ziel hat die Sicherheit von Informationen in Organisationen sicherzustellen (vgl. ISO 27001, siehe 1.6.4. Referenzen). Maßgebend für den Betrieb der EBCA sind die betriebsinternen Sicherheitsrichtlinien und Standards des Teilnehmers, welche sich dabei an ISO/IEC 27001 orientieren können (siehe Begriff Security Policy).
<b>KeyUsage (in Bezug auf CA-Zertifikate)</b>	In der Zertifikatserweiterung "KeyUsage" werden die Nutzungseigenschaften des öffentlichen Schlüssels festgelegt. CAs müssen bei der Definition der Zertifikatserweiterungen die Konformitätskriterien der EBCA berücksichtigen. Die "KeyUsage" ist dabei auf kritisch zu setzen.
<b>LDAP</b>	"Lightweight Directory Access Protocol (LDAP) ist ein TCP/IP-basiertes Directory-Zugangsprotokoll, das sich im Internet und in Intranets als Standardlösung für den Zugriff auf Netzwerk-Verzeichnisdienste für Datenbanken, E-Mails, Speicherbereiche und andere Ressourcen etabliert hat" (vgl. ITWissen, siehe 1.6.4. Referenzen). Die EBCA stellt einen zentralisierten LDAP-Verzeichnisdienst zur Verfügung um die Verteilung der Zertifikate zu gewährleisten. Wird das LDAP-Verzeichnis eingebunden, können Nutzer aus ihren Anwendungen Verschlüsselungszertifikate von EBCA-Teilnehmern anfordern und Daten mit diesen Personen direkt verschlüsselt austauschen.
<b>Object Identifier</b>	Der Object Identifier (OID) ist eine Folge von Zeichen und Ziffern und dient zur Beschreibung und weltweit eindeutigen Kennzeichnung von abstrakten Objekten in der Informatik. Im Sinne der EBCA wird empfohlen, die OIDs der zugehörigen CPs im X.509-Zertifikat in der nicht kritischen Erweiterung des Attributs "certificatePolicies" einzutragen. Der OID für dieses Dokument lautet: 1.3.6.1.4.1.20351.1.2.1.



<b>OCSP</b>	<p>Das Online Certificate Status Protocol (OCSP) ist ein Protokoll zur Online-Überprüfung des aktuellen Zustands eines Zertifikats. Mit der Statusabfrage über OCSP wird ermittelt, ob ein Zertifikat noch gültig oder gesperrt ist. Dem Verfahren nach richtet ein OCSP-Client eine Statusanfrage an den OCSP-Server, der diese mit gut, gesperrt oder unbekannt beantwortet. Jeder EBCA-Teilnehmer muss ein Verfahren (z.B. CRL, LDAP, OCSP) zur Überprüfung der Gültigkeit von Zertifikaten anbieten.</p>
<b>Public Key Infrastructure</b>	<p>Unter einer Public-Key-Infrastruktur (PKI) wird eine Umgebung verstanden, "in der Services zur Verschlüsselung und zur digitalen Signatur auf Basis von Public-Key-Verfahren bereitgestellt werden. Bei dieser Sicherheitsstruktur wird der öffentliche Schlüssel eines Zertifikatnehmers (...) mit den entsprechenden Identifikationsmerkmalen durch eine digitale Signatur von einer Zertifizierungsinstanz (...) autorisiert" (vgl. ITWissen, siehe 1.6.4. Referenzen).</p>
<b>Security Policy</b>	<p>Die Security Policy ist ein verbindliches Dokument zur Beschreibung der Sicherheitspolitik einer Organisation. Dieses Regelwerk enthält "die Richtlinien und Vorschriften, die die Personen beachten müssen, die Zugang zu Datenbeständen, Systemen und Ressourcen haben. In ihr werden die Regeln und Verfahrensweisen festgelegt, nach denen die Datenübermittlung, -verarbeitung und -speicherung erfolgen. Die Sicherheitspolitik berücksichtigt personelle, technische, organisatorische und rechtliche Einflussfaktoren" (vgl. ITWissen, siehe 1.6.4. Referenzen). Der sichere Umgang mit kryptographischem Schlüsselmaterial für die PKI kann arbeitsrechtlich verbindlich in einer Security Policy auch außerhalb der CP geregelt werden. In der Neufassung des Standards ISO 27001:2013 ist der Umgang mit Kryptographie zu einem eigenständigen Control geworden, so dass sich dies erst recht anbietet.</p>
<b>Registration Authority</b>	<p>Die "Registration Authority (RA) ist eine optionale Instanz innerhalb einer Sicherheitsinfrastruktur (PKI). Sie arbeitet eng mit der Certification Authority (CA) zusammen und ist zuständig für das sichere identifizieren und registrieren der User. Sie überprüft die Identität des Zertifikatnehmers(...), sendet den Antrag an die CA "und übergibt die persönliche Identifikationsnummer (PIN), die sie von der CA "erhält, an den Zertifikatnehmer" (vgl. ITWissen, siehe 1.6.4. Referenzen). Teilnehmer-RAs der EBCA können innerhalb oder außerhalb des Unternehmens/ der Organisation des EBCA-Teilnehmers angesiedelt sein und gewährleisten im Rahmen ihrer Sicherheitsrichtlinie eine zuverlässige Identifizierung und Authentisierung des Antragstellers.</p>
<b>Registrierungsprozess</b>	<p>Die Registrierung ist die Feststellung der Identität im Personalisierungsprozess in einer Registration Authority (RA) und signierte Weitergabe der Daten über einen sicheren Kanal an das Trustcenter. Dies ist Voraussetzung für die Antragstellung. Dem Teilnehmer im Verfahren für digitale Signaturen wird dabei ein geeigneter, eindeutiger Name zugewiesen. Vor einer EBCA-konformen Registrierung sind die Zertifikatsnehmer zuverlässig nach einem dokumentierten Prozess zu identifizieren. Die Registrierung muss ebenfalls ein dokumentierter Prozess sein.</p>
<b>Relying Parties</b>	<p>Relying Parties sind Zertifikatsnutzer, d.h. alle Personen und Organisationen, die Zertifikate von Zertifikatsnehmern nutzen und Zugang zu den Diensten der EBCA haben. Zertifikatsnutzer von EBCA-Teilnehmern können den EBCA-Verzeichnisdienst dazu nutzen, öffentliche Schlüssel von EBCA-Teilnehmern über den EBCA-Verzeichnisdienst zu suchen und herunterzuladen. Dieser kann auch als LDAP-Verzeichnis in den E-Mail Client eingebunden werden.</p>

<b>RFC 822</b>	Im RFC 822-Standard wird die Syntax und das Format von E-Mail-Nachrichten beschrieben. Eine E-Mail besteht aus einem Body der die zu transportierenden Nachricht enthält und einem Header, der Informationen unter anderem über den Absender, Empfänger, das Datum und den Betreff beinhaltet. Um eine EBCA-konforme Identifizierung und Authentifizierung von Zertifikaten sicherzustellen soll die Anwendung der Namensregeln gemäß des RFC 822 erfolgen.
<b>RFC 3647</b>	Bei dem Internet-Standard RFC 3647 handelt es sich um das allgemein anerkannte Rahmenwerk, welches die Zertifizierung einer PKI und deren CP nach dem X.509-Standard (Erstellung digitaler Zertifikate) der Internationalen Telekommunikationsunion (ITU) beschreibt. Die CPs der EBCA, sowie deren Mitglieder, orientieren sich am RFC 3647 und ermöglichen dabei eine nach außen transparente und vergleichbare Darstellung der Sicherheitsstandards der innerhalb der EBCA betriebenen PKIs.
<b>Subject-DistinguishedName</b>	Der Eintrag "SubjectDistinguishedName" (Subject DN) ist der Name eines ausgestellten Zertifikates und identifiziert eindeutig den Zertifikatsnehmer. Die Eindeutigkeit von "Subject DNs" ist gegeben, wenn niemals zwei oder mehr unterschiedliche Entitäten den gleichen "Subject DN" zugewiesen bekommen. Bei der EBCA müssen Namensregeln für den "SubjectDistinguishedName" nach dem X.501-Standard definiert sein.
<b>S/MIME</b>	Die Secure/Multipurpose Internet Mail Extensions (S/MIME) ermöglicht das sichere Versenden und den sicheren Empfang von E-Mails oder anderen MIME-basierten Nachrichten (z.B. AS2). S/MIME "ist eine gesicherte Variante des MIME-Protokolls mit der die Vertraulichkeit, Authentizität und die Datenintegrität von Mail-Clients sichergestellt wird" (vgl. ITWissen, siehe 1.6.4. Referenzen).
<b>Technische Interoperabilität</b>	Technische Interoperabilität ist neben der Vergleichbarkeit der Sicherheitsniveaus und geeignete Mindeststandards ein Kriterium, welches neue EBCA-Teilnehmer erfüllen müssen. Dazu werden EBCA- Interoperabilitätstests durchgeführt, die mit einem positiven Ergebnis abgeschlossen werden müssen.
<b>Technische Konformität</b>	Die EBCA bietet eine Plattform für die technische Konformität durch Profilierung des technischen Standards Common PKI sowie für die Durchführung von Tests zur Feststellung gegenseitiger Interoperabilität. Die technische Konformität wird im Rahmen der EBCA-Interoperabilitätstests nachgewiesen.
<b>Teilnehmer Certificate Policy</b>	In der Teilnehmer Certificate Policy (Teilnehmer-CP) erklärt der EBCA-Teilnehmer (Teilnehmer), dass seine CA den Vorgaben und Anforderungen dieser CP der EBCA entspricht, er eine eigene Teilnehmer-CP erstellt hat, die die Vorgaben der EBCA-CP umsetzt und der Teilnehmer den notwendigen Interoperabilitätstest erfolgreich bestanden hat.
<b>Trust Service Provider</b>	Ein Trust Service Provider (TSP) / Certification Service Provider (CSP), bietet Dienstleistungen in Bezug zur Erstellung und Nutzung elektronischer Zertifikate an. TSP stellt im Kontext mit digitalen Zertifikaten einen Überbegriff dar und umfasst alle Dienstleister, welche Leistungen in Bezug auf elektronische Zertifizierungen erbringen.
<b>X.509 konforme Zertifikate</b>	X.509 konforme Zertifikate sind nach dem X.509-Standard der Internationalen Telekommunikation Union (ITU) erstellte digitaler Zertifikate aus denen "die Namen und die digitale Signatur des Ausstellers hervorgehen. (...) Bei diesen nach X.509 standardisierten Zertifikaten kann es sich auch um E-Mail-Zertifikate handeln, die der sicheren Übertragung von E-Mails und Dateien dienen und auch zur Identifikation gegenüber Websites benutzt werden" (vgl. ITWissen, siehe 1.6.4. Referenzen). Teilnehmerzertifikate der EBCA müssen konform zum Standard X.509 v3 (Typ 0x2) sein.

