

TeleTrust Deutschland e.V.



Zertifikatsrichtlinie (Certificate Policy)

für Mitglieder der

European Bridge-CA

Version 1.04
20. Januar 2009

Dieses Dokument unterliegt dem Copyright von TeleTrust Deutschland e.V. Vervielfältigung oder auszugsweise Vervielfältigung sind nicht ohne Verweis auf dieses Dokument erlaubt.

Inhaltsverzeichnis

| | | |
|-------|--|----|
| 1 | Einleitung | 8 |
| 1.1 | Überblick | 8 |
| 1.1.1 | Ziel dieser Richtlinie | 8 |
| 1.1.2 | RFC 3647 Struktur | 9 |
| 1.1.3 | Konventionen | 9 |
| 1.1.4 | Gültigkeit | 9 |
| 1.2 | Name und Kennzeichnung des Dokuments | 9 |
| 1.3 | PKI-Teilnehmer | 10 |
| 1.3.1 | Zertifizierungsstellen | 10 |
| 1.3.2 | Registrierungsstellen | 10 |
| 1.3.3 | Zertifikatsnehmer | 10 |
| 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 | 11 |
| 1.5.1 | Zuständigkeit für das Dokument | 11 |
| 1.5.2 | Ansprechpartner/Kontaktperson/Sekretariat | 11 |
| 1.5.3 | Pflege dieser Richtlinie | 11 |
| 1.5.4 | Annahmeverfahren für Teilnehmer-CP | 11 |
| 1.5.5 | Zuständiger für die Anerkennung einer CP in Hinblick auf diese CP | 12 |
| 1.6 | Begriffe und Abkürzungen | 12 |
| 1.6.1 | Deutsche Begriffe | 12 |
| 1.6.2 | Englische Begriffe | 12 |
| 1.6.3 | Abkürzungen | 12 |
| 1.6.4 | Referenzen | 12 |
| 2 | Verantwortlichkeit für Verzeichnisse und Veröffentlichungen | 13 |
| 2.1 | Verzeichnisse | 13 |
| 2.2 | Veröffentlichung von Informationen zur Zertifikatserstellung | 13 |
| 2.3 | Zeitpunkt und Häufigkeit von Veröffentlichungen | 13 |
| 2.4 | Zugriffskontrollen auf Verzeichnisse | 13 |
| 3 | Identifizierung und Authentifizierung | 14 |
| 3.1 | Namensregeln | 14 |
| 3.1.1 | Arten von Namen | 14 |
| 3.1.2 | Notwendigkeit für aussagefähige Namen | 14 |
| 3.1.3 | Anonymität oder Pseudonymität von Zertifikatsnehmern | 14 |
| 3.1.4 | Regeln für die Interpretation verschiedener Namensformen | 14 |
| 3.1.5 | Eindeutigkeit von Namen | 14 |
| 3.1.6 | Anerkennung, Authentifizierung und Rolle von Markennamen | 14 |
| 3.2 | Erstmalige Überprüfung der Identität | 14 |
| 3.2.1 | Methoden zur Überprüfung des Besitzes des privaten Schlüssels | 14 |
| 3.2.2 | Authentifizierung von Organisationszugehörigkeiten | 14 |
| 3.2.3 | Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers | 14 |
| 3.2.4 | Ungeprüfte Zertifikatsnehmerangaben | 15 |
| 3.2.5 | Prüfung der Berechtigung zur Antragstellung | 15 |

| | | |
|-------|---|----|
| 3.2.6 | Kriterien zur „Interoperation“ (Zusammenwirkung/Wechselwirkung) | 15 |
| 3.3 | Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Rekeying)..... | 15 |
| 3.3.1 | Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung | 15 |
| 3.3.2 | Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen | 15 |
| 3.4 | Identifizierung und Authentifizierung von Sperranträgen..... | 15 |
| 4 | Betriebsanforderungen..... | 16 |
| 4.1 | Zertifikatsantrag | 16 |
| 4.1.1 | Wer kann einen Zertifikatsantrag stellen?..... | 16 |
| 4.1.2 | Registrierungsprozess und Zuständigkeiten..... | 16 |
| 4.2 | Verarbeitung des Zertifikatsantrags..... | 16 |
| 4.2.1 | Durchführung der Identifizierung und Authentifizierung..... | 16 |
| 4.2.2 | Annahme oder Ablehnung von Zertifikatsanträgen..... | 16 |
| 4.2.3 | Fristen für die Bearbeitung von Zertifikatsanträgen | 16 |
| 4.3 | Zertifikatsausgabe | 16 |
| 4.3.1 | Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten | 16 |
| 4.3.2 | Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats durch die CA | 16 |
| 4.4 | Zertifikatsannahme | 16 |
| 4.4.1 | Verhalten für eine Zertifikatsannahme | 16 |
| 4.4.2 | Veröffentlichung des Zertifikats durch die CA..... | 17 |
| 4.4.3 | Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats | 17 |
| 4.5 | Verwendung des Schlüsselpaares und des Zertifikats | 17 |
| 4.5.1 | Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer | 17 |
| 4.5.2 | Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer | 17 |
| 4.6 | Zertifikatserneuerung..... | 17 |
| 4.6.1 | Bedingungen für eine Zertifikatserneuerung..... | 17 |
| 4.6.2 | Wer darf eine Zertifikatserneuerung beantragen? | 17 |
| 4.6.3 | Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung | 17 |
| 4.6.4 | Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats | 18 |
| 4.6.5 | Verhalten für die Annahme einer Zertifikatserneuerung | 18 |
| 4.6.6 | Veröffentlichung der Zertifikatserneuerung durch die CA..... | 18 |
| 4.6.7 | Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats | 18 |
| 4.7 | Zertifizierung nach Schlüsselerneuerung | 18 |
| 4.7.1 | Bedingungen für eine Zertifizierung nach Schlüsselerneuerung | 18 |
| 4.7.2 | Wer darf Zertifikate für Schlüsselerneuerungen beantragen? | 18 |
| 4.7.3 | Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen | 18 |
| 4.7.4 | Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats..... | 18 |
| 4.7.5 | Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen..... | 18 |
| 4.7.6 | Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA..... | 18 |
| 4.7.7 | Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats..... | 19 |
| 4.8 | Zertifikatsänderung..... | 19 |
| 4.8.1 | Bedingungen für eine Zertifikatsänderung..... | 19 |
| 4.8.2 | Wer darf eine Zertifikatsänderung beantragen? | 19 |

| | | |
|--------|---|----|
| 4.8.3 | Bearbeitung eines Antrags auf Zertifikatsänderung..... | 19 |
| 4.8.4 | Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats | 19 |
| 4.8.5 | Verhalten für die Annahme einer Zertifikatsänderung | 19 |
| 4.8.6 | Veröffentlichung der Zertifikatsänderung durch die CA | 19 |
| 4.8.7 | Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines neuen Zertifikats | 19 |
| 4.9 | Sperrung und Suspendierung von Zertifikaten | 20 |
| 4.9.1 | Bedingungen für eine Sperrung | 20 |
| 4.9.2 | Wer kann eine Sperrung beantragen?..... | 20 |
| 4.9.3 | Verfahren für einen Sperrantrag | 20 |
| 4.9.4 | Fristen für einen Sperrantrag | 20 |
| 4.9.5 | Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch den Zertifizierungsdiensteanbieter..... | 20 |
| 4.9.6 | Verfügbare Methoden zum Prüfen von Sperrinformationen | 20 |
| 4.9.7 | Frequenz der Veröffentlichung von Sperrlisten..... | 20 |
| 4.9.8 | Maximale Latenzzeit für Sperrlisten..... | 20 |
| 4.9.9 | Verfügbarkeit von Online-Sperrinformationen..... | 20 |
| 4.9.10 | Anforderungen zur Online-Prüfung von Sperrinformationen..... | 20 |
| 4.9.11 | Andere Formen zur Anzeige von Sperrinformationen..... | 21 |
| 4.9.12 | Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels..... | 21 |
| 4.9.13 | Bedingungen für eine Suspendierung..... | 21 |
| 4.9.14 | Wer kann eine Suspendierung beantragen? | 21 |
| 4.9.15 | Verfahren für Anträge auf Suspendierung | 21 |
| 4.9.16 | Begrenzungen für die Dauer von Suspendierungen..... | 21 |
| 4.10 | Statusabfragedienst für Zertifikate..... | 21 |
| 4.10.1 | Funktionsweise des Statusabfragedienstes..... | 21 |
| 4.10.2 | Verfügbarkeit des Statusabfragedienstes | 21 |
| 4.10.3 | Optionale Leistungen | 21 |
| 4.11 | Kündigung durch den Zertifikatsnehmer..... | 21 |
| 4.12 | Schlüssel hinterlegung und Wiederherstellung | 21 |
| 4.12.1 | Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel..... | 21 |
| 4.12.2 | Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln | 21 |
| 5 | Nicht-technische Sicherheitsmaßnahmen..... | 22 |
| 5.1 | Bauliche Sicherheitsmaßnahmen | 23 |
| 5.1.1 | Lage und Gebäude | 23 |
| 5.1.2 | Zugang..... | 23 |
| 5.1.3 | Strom, Heizung und Klimaanlage | 23 |
| 5.1.4 | Wassergefährdung..... | 23 |
| 5.1.5 | Brandschutz | 23 |
| 5.1.6 | Lager und Archiv..... | 23 |
| 5.1.7 | Müllbeseitigung | 23 |
| 5.1.8 | Desaster Backup..... | 23 |
| 5.2 | Verfahrensvorschriften..... | 23 |
| 5.2.1 | Rollenkonzept | 23 |
| 5.2.2 | Mehraugenprinzip | 23 |
| 5.2.3 | Rollenausschlüsse | 23 |
| 5.3 | Personalkontrolle | 23 |
| 5.3.1 | Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit..... | 23 |
| 5.3.2 | Methoden zur Überprüfung der Rahmenbedingungen | 23 |
| 5.3.3 | Anforderungen an Schulungen | 23 |

| | | |
|-------|---|----|
| 5.3.4 | Häufigkeit von Schulungen und Belehrungen..... | 23 |
| 5.3.5 | Häufigkeit und Folge von Job-Rotation..... | 23 |
| 5.3.6 | Maßnahmen bei unerlaubten Handlungen..... | 23 |
| 5.3.7 | Anforderungen an freie Mitarbeiter | 23 |
| 5.3.8 | Dokumente, die dem Personal zur Verfügung gestellt werden müssen | 23 |
| 5.4 | Überwachungsmaßnahmen..... | 23 |
| 5.4.1 | Arten von aufgezeichneten Ereignissen | 24 |
| 5.4.2 | Häufigkeit der Bearbeitung der Aufzeichnungen | 24 |
| 5.4.3 | Aufbewahrungszeit von Aufzeichnungen..... | 24 |
| 5.4.4 | Sicherung der Aufzeichnungen..... | 24 |
| 5.4.5 | Datensicherung der Aufzeichnungen..... | 24 |
| 5.4.6 | Speicherung der Aufzeichnungen (intern / extern) | 24 |
| 5.4.7 | Benachrichtigung der Ereignisauslöser | 24 |
| 5.4.8 | Verwundbarkeitsabschätzungen..... | 24 |
| 5.5 | Archivierung von Aufzeichnungen | 24 |
| 5.5.1 | Arten von archivierten Aufzeichnungen | 24 |
| 5.5.2 | Aufbewahrungsfristen für archivierte Daten..... | 24 |
| 5.5.3 | Sicherung des Archivs | 24 |
| 5.5.4 | Datensicherung des Archivs | 24 |
| 5.5.5 | Anforderungen zum Zeitstempeln von Aufzeichnungen | 24 |
| 5.5.6 | Archivierung (intern / extern)..... | 24 |
| 5.5.7 | Verfahren zur Beschaffung und Verifikation von Archivinformationen..... | 24 |
| 5.6 | Schlüsselwechsel beim Zertifizierungsdiensteanbieter (CSP)..... | 24 |
| 5.7 | Kompromittierung und Geschäftweiterführung beim Zertifizierungsdiensteanbieter (CSP) | 24 |
| 5.7.1 | Behandlung von Vorfällen und Kompromittierungen | 24 |
| 5.7.2 | Rechnerressourcen-, Software- und/oder Datenkompromittierung | 24 |
| 5.7.3 | Kompromittierung des privaten Schlüssels des Zertifizierungsdiensteanbieter (CSP) | 24 |
| 5.7.4 | Möglichkeiten zur Geschäftweiterführung nach einer Kompromittierung..... | 24 |
| 5.8 | Schließung eines Zertifizierungsdiensteanbieter (CSP) oder einer Registrierungsstelle | 24 |
| 6 | Technische Sicherheitsmaßnahmen..... | 25 |
| 6.1 | Erzeugung und Installation von Schlüsselpaaren..... | 25 |
| 6.1.1 | Erzeugung von Schlüsselpaaren | 25 |
| 6.1.2 | Lieferung privater Schlüssel an Zertifikatsnehmer..... | 25 |
| 6.1.3 | Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber | 25 |
| 6.1.4 | Lieferung öffentlicher Schlüssel des Zertifizierungsdiensteanbieter an Zertifikatsnutzer | 25 |
| 6.1.5 | Schlüssellängen..... | 25 |
| 6.1.6 | Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle | 26 |
| 6.1.7 | Schlüsselverwendungen..... | 26 |
| 6.2 | Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module | 26 |
| 6.2.1 | Standards und Sicherheitsmaßnahmen für kryptographische Module | 26 |
| 6.2.2 | Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)..... | 26 |
| 6.2.3 | Hinterlegung privater Schlüssel | 26 |
| 6.2.4 | Sicherung privater Schlüssel | 26 |
| 6.2.5 | Archivierung privater Schlüssel..... | 26 |
| 6.2.6 | Transfer privater Schlüssel in oder aus kryptographischen Modulen | 26 |
| 6.2.7 | Speicherung privater Schlüssel in kryptographischen Modulen | 26 |
| 6.2.8 | Aktivierung privater Schlüssel..... | 26 |
| 6.2.9 | Deaktivierung privater Schlüssel..... | 26 |

| | | |
|--------|---|----|
| 6.2.10 | Zerstörung privater Schlüssel | 26 |
| 6.2.11 | Beurteilung kryptographischer Module | 26 |
| 6.3 | Andere Aspekte des Managements von Schlüsselpaaren | 26 |
| 6.3.1 | Archivierung öffentlicher Schlüssel | 26 |
| 6.3.2 | Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren | 26 |
| 6.4 | Aktivierungsdaten | 26 |
| 6.4.1 | Aktivierungsdaten | 26 |
| 6.4.2 | Schutz von Aktivierungsdaten..... | 26 |
| 6.5 | Sicherheitsmaßnahmen in den Rechneranlagen..... | 26 |
| 6.5.1 | Spezifische technische Sicherheitsanforderungen in den Rechneranlagen | 26 |
| 6.5.2 | Beurteilung von Computersicherheit..... | 26 |
| 6.6 | Technische Maßnahmen während des Life Cycles | 27 |
| 6.6.1 | Sicherheitsmaßnahmen bei der Entwicklung..... | 27 |
| 6.6.2 | Sicherheitsmaßnahmen beim Computermanagement | 27 |
| 6.6.3 | Sicherheitsmaßnahmen während der Life Cycles | 27 |
| 6.7 | Sicherheitsmaßnahmen für Netze | 27 |
| 6.8 | Zeitstempel | 27 |
| 7 | Profile von Zertifikaten, Sperrlisten und OCSP | 28 |
| 7.1 | Zertifikatsprofile | 28 |
| 7.1.1 | Versionsnummern..... | 28 |
| 7.1.2 | Zertifikatserweiterungen..... | 28 |
| 7.1.3 | Algorithmen OIDs..... | 28 |
| 7.1.4 | Namensformate | 28 |
| 7.1.5 | Namensbeschränkungen | 28 |
| 7.1.6 | OIDs der Zertifikatsrichtlinien..... | 28 |
| 7.1.7 | Nutzung der Erweiterung „Policy Constraints“ | 28 |
| 7.1.8 | Syntax und Semantik von „Policy Qualifiers“ | 28 |
| 7.1.9 | Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie..... | 29 |
| 7.2 | Sperrlistenprofile..... | 29 |
| 7.2.1 | Versionsnummer(n) | 29 |
| 7.2.2 | Erweiterungen von Sperrlisten und Sperrlisteneinträgen..... | 29 |
| 7.3 | Profile des Statusabfragedienstes (OCSP) | 29 |
| 7.3.1 | Versionsnummer(n) | 29 |
| 7.3.2 | OCSP Erweiterungen..... | 29 |
| 8 | Überprüfungen und andere Bewertungen..... | 30 |
| 8.1 | Häufigkeit und Bedingungen für Überprüfungen | 30 |
| 8.2 | Identität/Qualifikation des Prüfers..... | 30 |
| 8.3 | Stellung des Prüfers zum Bewertungsgegenstand..... | 30 |
| 8.4 | Durch Überprüfungen abgedeckte Themen | 30 |
| 8.5 | Reaktionen auf Unzulänglichkeiten | 30 |
| 8.6 | Information über Bewertungsergebnisse | 30 |
| 9 | Andere finanzielle und rechtliche Angelegenheiten | 31 |
| 9.1 | Preise..... | 32 |
| 9.1.1 | Preise für Zertifikate oder Zertifikatserneuerungen..... | 32 |
| 9.1.2 | Preise für den Zugriff auf Zertifikate..... | 32 |
| 9.1.3 | Preise für Sperrungen oder Statusinformationen..... | 32 |
| 9.1.4 | Preise für andere Dienstleistungen..... | 32 |
| 9.2 | Finanzielle Zuständigkeiten | 32 |
| 9.2.1 | Versicherungsdeckung | 32 |
| 9.2.2 | Andere Posten | 32 |
| 9.2.3 | Versicherung oder Gewährleistung für Endnutzer | 32 |
| 9.3 | Vertraulichkeitsgrad von Geschäftsdaten..... | 32 |
| 9.3.1 | Definition von vertraulichen Informationen..... | 32 |

| | | |
|--------|---|----|
| 9.3.2 | Informationen, die nicht zu den vertraulichen Informationen gehören | 32 |
| 9.3.3 | Zuständigkeiten für den Schutz vertraulicher Informationen..... | 32 |
| 9.4 | Datenschutz von Personendaten..... | 32 |
| 9.4.1 | Datenschutzkonzept | 32 |
| 9.4.2 | Als persönlich behandelte Daten | 32 |
| 9.4.3 | Daten, die nicht als persönlich behandelt werden | 32 |
| 9.4.4 | Zuständigkeiten für den Datenschutz | 32 |
| 9.4.5 | Hinweis und Einwilligung zur Nutzung persönlicher Daten..... | 32 |
| 9.4.6 | Auskunft gemäß rechtlicher oder staatlicher Vorschriften | 32 |
| 9.4.7 | Andere Bedingungen für Auskünfte | 32 |
| 9.5 | Geistiges Eigentumsrecht..... | 32 |
| 9.6 | Zusicherungen und Garantien | 32 |
| 9.6.1 | Zusicherungen und Garantien der CA | 33 |
| 9.6.2 | Zusicherungen und Garantien der RA | 33 |
| 9.6.3 | Zusicherungen und Garantien der Zertifikatsnehmer | 33 |
| 9.6.4 | Zusicherungen und Garantien der Zertifikatsnutzer..... | 33 |
| 9.6.5 | Zusicherungen und Garantien anderer PKI-Teilnehmer | 33 |
| 9.7 | Haftungsausschlüsse | 33 |
| 9.8 | Haftungsbeschränkungen..... | 33 |
| 9.9 | Schadensersatz | 33 |
| 9.10 | Gültigkeitsdauer und Beendigung..... | 33 |
| 9.10.1 | Gültigkeitsdauer | 33 |
| 9.10.2 | Beendigung..... | 33 |
| 9.10.3 | Auswirkung der Beendigung und Weiterbestehen..... | 33 |
| 9.11 | Individuelle Mitteilungen und Absprachen mit Teilnehmern | 33 |
| 9.12 | Ergänzungen | 33 |
| 9.12.1 | Verfahren für Ergänzungen..... | 33 |
| 9.12.2 | Benachrichtigungsmechanismen und –fristen | 33 |
| 9.12.3 | Bedingungen für OID Änderungen..... | 33 |
| 9.13 | Verfahren zur Schlichtung von Streitfällen..... | 33 |
| 9.14 | Zugrunde liegendes Recht..... | 33 |
| 9.15 | Einhaltung geltenden Rechts..... | 33 |
| 9.16 | Sonstige Bestimmungen..... | 33 |
| 9.16.1 | Vollständigkeitserklärung | 33 |
| 9.16.2 | Abgrenzungen..... | 33 |
| 9.16.3 | Salvatorische Klausel..... | 33 |
| 9.16.4 | Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht) | 34 |
| 9.16.5 | Höhere Gewalt | 34 |
| 9.17 | Andere Bestimmungen | 34 |
| 10 | Anhang | 35 |
| 10.1 | Begriffsdefinitionen CP / CPS / PDS | 35 |
| 10.1.1 | CP (Certificate Policy)..... | 35 |
| 10.1.2 | CPS (Certification Practice Statement)..... | 35 |
| 10.1.3 | PDS (PKI Disclosure Statement) | 35 |
| 10.2 | Wichtige Begriffe in einer Public Key Infrastruktur..... | 36 |

1 Einleitung

1.1 Überblick

Diese Zertifikatsrichtlinie (engl. Certificate Policy CP) ist gerichtet an Teilnehmer der European Bridge-CA (EB-CA). Sie enthält Vorgaben und Anforderungen an die teilnehmenden Public Key Infrastructure (PKI) 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 EB-CA dienen. Diese CP orientiert sich am RFC 3647.

Der EB-CA 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.¹

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

Diese Zertifikatsrichtlinie beschreibt Sicherheitsanforderungen an den Betrieb von Zertifizierungsstellen für die Ausstellung und Nutzung von X.509 konformen Zertifikaten. Darüber hinaus definiert die Richtlinie für Dritte einen Grundschatz 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 EB-CA bindend. Bestandsmitgliedern steht ein Übergangszeitraum zur Umsetzung und Dokumentation bis zum 1.1.2008 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 EB-CA 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 EB-CA 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 EB-CA Vorgaben für Mindeststandards an Sicherheit zum Betrieb einer EB-CA konformen PKI gegeben. Der Aufbau nach RFC

¹ Die technische Konformität zur Erreichung von Interoperabilität am Beispiel für sichere E-Mail wird im Dokument „Testspezifikation Interoperabilität und Funktionalität für den Austausch sicherer E-Mails mit Zertifikaten unter der European Bridge-CA“ [EB-CA S/MIME] beschrieben.

3647 ermöglicht eine nach Außen transparente und vergleichbare Darstellung der Sicherheitsstandards der innerhalb der EB-CA betriebenen PKIen.

Jedes Mitglied der EB-CA 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)², 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.

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 EB-CA
- **soll, (sollte)**
Vorgabe der EB-CA, 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 BSI³ oder nach ISO/IEC 17799⁴ 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 ab 1.1.2006 bindend für Mitglieder der EB-CA. Für Bestandsmitglieder besteht ein Übergangszeitraum zur Umsetzung bis zum 1.1.2008.

1.2 Name und Kennzeichnung des Dokuments

Diese Zertifikatsrichtlinie trägt den Titel:

² Früher wurden die Mindestanforderungen an die teilnehmende PKI innerhalb der Selbsterklärung formuliert. Nun verweist die Selbsterklärung auf diese CP.

³ Bundesamt für Sicherheit der Informationstechnik (BSI), IT-Grundschutzhandbuch, siehe <http://www.bsi.de/gshb>

⁴ ISO-17799, <http://www.iso.org>

Zertifikatsrichtlinie für Mitglieder der European Bridge-CA,

Version: 1.02 - Datum: 18. August 2006

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 Zertifizierungsdienstleister beauftragt haben.

1.3.1 Zertifizierungsstellen

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

1.3.2 Registrierungsstellen

Registrierungsstellen (RAs) sind Stellen, die Registrierungen für Zertifikatsnehmer durchführen. Teilnehmer-RA's können innerhalb oder außerhalb des Unternehmens des Teilnehmers angesiedelt sein.

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer sind natürliche oder juristische Personen oder von diesen verantwortete technische Entitäten (Maschinen oder Programme). Die verantwortlichen natürlichen oder juristischen Personen haben ein Vertragsverhältnis mit der Teilnehmer-CA über die Ausstellung von Zertifikaten.⁵

1.3.4 Zertifikatsnutzer

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

1.3.5 Andere Teilnehmer

Teilnehmer, die keine Verpflichtungen gegenüber der EB-CA eingegangen sind, sind nicht Bestandteil dieser Richtlinie.

1.4 Verwendung von Zertifikaten**1.4.1 Erlaubte Verwendungen von Zertifikaten**

Der EB-CA 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

⁵ Es kann im Zertifikat einer juristischen oder natürlichen Person eine Organisation oder Funktionseinheit zugeordnet werden.

1.5 Pflege der Richtlinie

1.5.1 Zuständigkeit für das Dokument

EB-CA Board
TeleTrusT Deutschland e.V.
Chausseestraße 17
D-10115 Berlin

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

European Bridge-CA
Serviceverantwortlicher
Chausseestraße 17
D-10115 Berlin
info@eb-ca.de
<http://www.bridge-ca.org>
Phone: +49-30-4005 4310
Fax: +49-30-4005 4311

1.5.3 Pflege dieser Richtlinie

Diese Richtlinie wird inhaltlich durch die Mitglieder der AG-Technik der EB-CA gepflegt. Eine inhaltliche Überprüfung erfolgt alle 2 Jahre und wird durch das Board der EB-CA 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-CP⁶

Der Teilnehmer beantragt die Aufnahme seiner CA in die EB-CA. Die Beantragung umfasst die Teilnahme am E-Mail Interoperabilitätstest der EB-CA, sowie eine Selbsterklärung. Im Einzelnen erklärt er:

- dass seine 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 EB-CA Teilnehmer im Rahmen einer Erklärung zur teilweisen Nicht-Konformität die Stellen, wo keine Entsprechung gegenüber dieser CP vorliegt.

Das Board der EB-CA 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 EB-CA anzuzeigen.

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

⁶ 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.

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 EB-CA 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 EB-CA.

1.6 Begriffe und Abkürzungen

Begriffe und Abkürzungen finden sich im Anhang.

1.6.1 Deutsche Begriffe

1.6.2 Englische Begriffe

1.6.3 Abkürzungen

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>.
- [EB-CA S/MIME] European Bridge-CA, "Sichere E-mail: Testspezifikation Interoperabilität und Funktionalität für den Austausch sicherer E-Mails mit Zertifikaten unter der European Bridge-CA",
Abrufbar unter <http://www.bridge-ca.org>.
- [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>.
- [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.

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Der Teilnehmer **muss** der EB-CA 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 Verzeichnisdienstleistungen 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 EB-CA 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 EB-CA als auch den anderen Teilnehmern zugänglich zu machen.

Der Teilnehmer stimmt einer Veröffentlichung seiner Teilnahme an der EB-CA und der Weitergabe seines Root-Zertifikates sowie untergeordneter CA-Zertifikate im Rahmen des EB-CA Verbundes zu.

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Der Teilnehmer **muss** Zeitpunkt und Häufigkeit der Veröffentlichung von Verzeichnis-Informationen (Sperrinformation, Zertifikatsliste) 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 EB-CA 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.

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Ein als Pseudonym oder anonym 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 Zertifikatshalters 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 EB-CA 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 Registrierungsstelle gewährleistet eine zuverlässige Identifizierung und Prüfung der Antragsdaten im Rahmen der Integritäts-, Authentizitäts- und Vertraulichkeits-

anforderungen 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 Antragsstellung **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 Registrierungsstelle gewährleistet eine zuverlässige Identifizierung und Prüfung der bisherigen Antragsdaten im Rahmen seiner Sicherheitsrichtlinie.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Registrierungsstelle 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 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 EB-CA 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 EB-CA teilnimmt, **muss** die EB-CA unverzüglich benachrichtigt werden.

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

Für Benutzerzertifikate gelten keine Vorgaben.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die Verantwortlichkeiten des Zertifikatsnehmers **müssen** durch den Zertifizierungsdiensteanbieter 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 Schlüsselpaares **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 EB-CA unverzüglich veröffentlicht werden.

Erneuerte Endnutzerzertifikate **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 EB-CA unverzüglich angezeigt werden.

Für Benutzerzertifikate gelten keine Vorgaben.

4.7 Zertifizierung nach Schlüsselerneuerung

4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung

Die Zertifizierungsstelle **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 EB-CA 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 EB-CA unverzüglich angezeigt werden.

Für Benutzerzertifikate gelten keine Vorgaben.

4.8 Zertifikatsänderung

4.8.1 Bedingungen für eine Zertifikatsänderung

Die Zertifizierungsstelle **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 EB-CA 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 EB-CA unverzüglich angezeigt werden.

Für Benutzerzertifikate gelten keine Vorgaben.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

Die Zertifizierungsstelle **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 Zertifizierungsstelle (CA) ist der EB-CA 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 Registrierungsstelle, als auch die Zertifizierungsstelle **müssen** das Verfahren für die Sperrung eines Zertifikates dokumentieren.

4.9.4 Fristen für einen Sperrantrag

Die Zertifizierungsstelle **soll** Fristen für einen Sperrantrag gegenüber dem Zertifikatsnehmer dokumentieren.

4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch den Zertifizierungdiensteanbieter

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 EB-CA entsprechen.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Die Frequenz der Veröffentlichung von Sperrlisten **muss** von der Zertifizierungsstelle 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 Zertifizierungsstelle 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. Der Statusabfragedienst **soll** interoperabel mit dem zentralisierten OCSP-Responder der EB-CA 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 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Im Fall einer Schlüsselhinterlegung **muss** der Zertifizierungsdiensteanbieter die Prozesse der Schlüsselhinterlegung dokumentieren. Diese **müssen** der eigenen Sicherheitsrichtlinie und dem aktuellen Stand der Technik entsprechen. Eine Schlüsselhinterlegung **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 (CSP)**
- Abschnitt 5.7 **Kompromittierung des privaten Schlüssels des Zertifizierungsdiensteanbieter (CSP)**
- Abschnitt 5.8 **Schließung eines Zertifizierungsdiensteanbieter (CSP) oder einer Registrierungsstelle**

-
- 5.1 Bauliche Sicherheitsmaßnahmen**
 - 5.1.1 Lage und Gebäude**
 - 5.1.2 Zugang**
 - 5.1.3 Strom, Heizung und Klimaanlage**
 - 5.1.4 Wassergefährdung**
 - 5.1.5 Brandschutz**
 - 5.1.6 Lager und Archiv**
 - 5.1.7 Müllbeseitigung**
 - 5.1.8 Desaster Backup**
 - 5.2 Verfahrensvorschriften**
 - 5.2.1 Rollenkonzept**
 - 5.2.2 Mehraugenprinzip**
 - 5.2.3 Rollenausschlüsse**
 - 5.2.4 Rollentrennung**
 - 5.3 Personalkontrolle**
 - 5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit**
 - 5.3.2 Methoden zur Überprüfung der Rahmenbedingungen**
 - 5.3.3 Anforderungen an Schulungen**
 - 5.3.4 Häufigkeit von Schulungen und Belehrungen**
 - 5.3.5 Häufigkeit und Folge von Job-Rotation**
 - 5.3.6 Maßnahmen bei unerlaubten Handlungen**
 - 5.3.7 Anforderungen an freie Mitarbeiter**
 - 5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen**
 - 5.4 Überwachungsmaßnahmen**

-
- 5.4.1 **Arten von aufgezeichneten Ereignissen**
 - 5.4.2 **Häufigkeit der Bearbeitung der Aufzeichnungen**
 - 5.4.3 **Aufbewahrungszeit von Aufzeichnungen**
 - 5.4.4 **Sicherung der Aufzeichnungen**
 - 5.4.5 **Datensicherung der Aufzeichnungen**
 - 5.4.6 **Speicherung der Aufzeichnungen (intern / extern)**
 - 5.4.7 **Benachrichtigung der Ereignisauslöser**
 - 5.4.8 **Verwundbarkeitsabschätzungen**
 - 5.5 **Archivierung von Aufzeichnungen**
 - 5.5.1 **Arten von archivierten Aufzeichnungen**
 - 5.5.2 **Aufbewahrungsfristen für archivierte Daten**
 - 5.5.3 **Sicherung des Archivs**
 - 5.5.4 **Datensicherung des Archivs**
 - 5.5.5 **Anforderungen zum Zeitstempeln von Aufzeichnungen**
 - 5.5.6 **Archivierung (intern / extern)**
 - 5.5.7 **Verfahren zur Beschaffung und Verifikation von Archivinformationen**
 - 5.6 **Schlüsselwechsel beim Zertifizierungsdiensteanbieter (CSP)**
 - 5.7 **Kompromittierung und Geschäftsführung beim Zertifizierungsdiensteanbieter (CSP)**
 - 5.7.1 **Behandlung von Vorfällen und Kompromittierungen**
 - 5.7.2 **Rechnerressourcen-, Software- und/oder Datenkompromittierung**
 - 5.7.3 **Verhalten bei Kompromittierung des privaten Schlüssels des Zertifizierungsdiensteanbieter (CSP)**
 - 5.7.4 **Möglichkeiten zur Geschäftsführung nach einer Kompromittierung**
 - 5.8 **Schließung eines Zertifizierungsdiensteanbieter (CSP) oder einer Registrierungsstelle**

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

6.1.1 Erzeugung von Schlüsselpaaren

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

6.1.4 Lieferung öffentlicher Schlüssel des Zertifizierungsdiensteanbieter an Zertifikatsnutzer

6.1.5 Schlüssellängen

Die verwendeten Schlüssellängen **sollten** sich am aktuellen Stand der Technik orientieren [ECRYPT, SigAlg].

-
- 6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle**
 - 6.1.7 Schlüsselverwendungen**
 - 6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module**
 - 6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module**
 - 6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)**
 - 6.2.3 Hinterlegung privater Schlüssel**
 - 6.2.4 Sicherung privater Schlüssel**
 - 6.2.5 Archivierung privater Schlüssel**
 - 6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen**
 - 6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen**
 - 6.2.8 Aktivierung privater Schlüssel**
 - 6.2.9 Deaktivierung privater Schlüssel**
 - 6.2.10 Zerstörung privater Schlüssel**
 - 6.2.11 Beurteilung kryptographischer Module**
 - 6.3 Andere Aspekte des Managements von Schlüsselpaaren**
 - 6.3.1 Archivierung öffentlicher Schlüssel**
 - 6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren**
 - 6.4 Aktivierungsdaten**
 - 6.4.1 Aktivierungsdaten**
 - 6.4.2 Schutz von Aktivierungsdaten**
 - 6.5 Sicherheitsmaßnahmen in den Rechneranlagen**
 - 6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen**
 - 6.5.2 Beurteilung von Computersicherheit**

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

6.6.3 Sicherheitsmaßnahmen während der Life Cycles

6.7 Sicherheitsmaßnahmen für Netze

6.8 Zeitstempel

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 Zertifizierungsstelle **muss** die Zertifikatserweiterungen definieren. Dabei **sollen** Konformitätskriterien der EB-CA 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 ISIS-MTT-Profilierung eingehalten werden (siehe [ISIS/MTT] ISIS/MTT Version 1.1, Part 1. Table 12: KeyUsage)

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

- Im SubjectAltName (rfc822Name, bevorzugt) oder
- Innerhalb des DistinguishedName (E=)
- In technischen Zertifikaten sollte der primäre Systemname im Distinguished Name (CN=) aufgenommen werden.

7.1.3 Algorithmen OIDs

Keine Vorgaben

7.1.4 Namensformate

Die CA **muss** Namensformate dokumentieren. Grundsätzlich **sollen** Konformitätskriterien der EB-CA 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** die 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 Zertifizierungsstelle eine OCSP-Statusprüfung zur Verfügung **muß** diese Erweiterung dokumentiert werden. Für die Definition dieser Erweiterungen **sollen** Konformitätskriterien der EB-CA 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.

8.1 Häufigkeit und Bedingungen für Überprüfungen

8.2 Identität/Qualifikation des Prüfers

8.3 Stellung des Prüfers zum Bewertungsgegenstand

8.4 Durch Überprüfungen abgedeckte Themen

8.5 Reaktionen auf Unzulänglichkeiten

8.6 Information über Bewertungsergebnisse

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.

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**
 - 9.1.2 Preise für den Zugriff auf Zertifikate**
 - 9.1.3 Preise für Sperrungen oder Statusinformationen**
 - 9.1.4 Preise für andere Dienstleistungen**
 - 9.1.5 Richtlinien für Rückerstattungen**
 - 9.2 Finanzielle Zuständigkeiten**
 - 9.2.1 Versicherungsdeckung**
 - 9.2.2 Andere Posten**
 - 9.2.3 Versicherung oder Gewährleistung für Endnutzer**
 - 9.3 Vertraulichkeitsgrad von Geschäftsdaten**
 - 9.3.1 Definition von vertraulichen Informationen**
 - 9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören**
 - 9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen**
 - 9.4 Datenschutz von Personendaten**
 - 9.4.1 Datenschutzkonzept**
 - 9.4.2 Als persönlich behandelte Daten**
 - 9.4.3 Daten, die nicht als persönlich behandelt werden**
 - 9.4.4 Zuständigkeiten für den Datenschutz**
 - 9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten**
 - 9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften**
 - 9.4.7 Andere Bedingungen für Auskünfte**
 - 9.5 Geistiges Eigentumsrecht**
 - 9.6 Zusicherungen und Garantien**

-
- 9.6.1 **Zusicherungen und Garantien der CA**
 - 9.6.2 **Zusicherungen und Garantien der RA**
 - 9.6.3 **Zusicherungen und Garantien der Zertifikatsnehmer**
 - 9.6.4 **Zusicherungen und Garantien der Zertifikatsnutzer**
 - 9.6.5 **Zusicherungen und Garantien anderer PKI-Teilnehmer**
 - 9.7 **Haftungsausschlüsse**
 - 9.8 **Haftungsbeschränkungen**
 - 9.9 **Schadensersatz**
 - 9.10 **Gültigkeitsdauer und Beendigung**
 - 9.10.1 **Gültigkeitsdauer**
 - 9.10.2 **Beendigung**
 - 9.10.3 **Auswirkung der Beendigung und Weiterbestehen**
 - 9.11 **Individuelle Mitteilungen und Absprachen mit Teilnehmern**
 - 9.12 **Ergänzungen**
 - 9.12.1 **Verfahren für Ergänzungen**
 - 9.12.2 **Benachrichtigungsmechanismen und –fristen**
 - 9.12.3 **Bedingungen für OID Änderungen**
 - 9.13 **Verfahren zur Schlichtung von Streitfällen**
 - 9.14 **Zugrunde liegendes Recht**
 - 9.15 **Einhaltung geltenden Rechts**
 - 9.16 **Sonstige Bestimmungen**
 - 9.16.1 **Vollständigkeitserklärung**
 - 9.16.2 **Abgrenzungen**
 - 9.16.3 **Salvatorische Klausel**

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

9.16.5 Höhere Gewalt

9.17 Andere Bestimmungen

10 Anhang

10.1 Begriffsdefinitionen CP / CPS / PDS

Dieses Dokument ist das CP der EB-CA. Das Dokument beschreibt Anforderungen für Teilnehmer der EB-CA. Der Teilnehmer bestätigt die Einhaltung der CP in seiner CPS.
Begriffsdefinition CP / CPS / PDS:

10.1.1 CP (Certificate Policy)

Generelle, verbindliche Anforderungen, unabhängig von der konkreten Ausprägung an den PKI-Betrieb des Teilnehmers. Die konkreten Aussagen werden in dem CPS beschrieben.

Das CP kann ganz oder in Teilen veröffentlicht werden (siehe auch PDS) und damit das Sicherheitsniveau der PKI charakterisieren.

Das CP der EB-CA ist konform zum RFC 3647.

10.1.2 CPS (Certification Practice Statement)

Beschreibung der konkreten Umsetzung des PKI-Betriebs im Rahmen des CP. Das CPS enthält normalerweise keine ablauforganisatorischen Festlegungen (diese befinden sich im Betriebskonzept bzw. in bereichsspezifischen Ergänzungen, die in der Regel nicht veröffentlicht werden).

CP / CPS wurden früher im RFC 2527 spezifiziert. Dieser wurde zum 1.12.2003 durch den RFC 3647 abgelöst.

10.1.3 PDS (PKI Disclosure Statement)

Die Anteile eines CP und/oder CPS, die man mit anderen austauschen möchte, um anderen Organisationen eine Entscheidung über die Vertrauenswürdigkeit der PKI zu ermöglichen.

Es enthält die wesentlichen Aussagen, die eine Einschätzung des Sicherheitsniveaus der betreffenden PKI ermöglichen.

10.2 Wichtige Begriffe in einer Public Key Infrastruktur

Begriffserklärungen:

| | |
|------------------------------|---|
| CA | Certification Authority. Technisch wird diese durch einen eindeutigen DistinguishedName identifiziert, welcher in den von dieser CA ausgestellten Zertifikaten als issuerDN erscheint. |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSP | Certificate Service Provider |
| DN | Distinguished Name |
| Eindeutigkeit Subject DNs | von Die Eindeutigkeit von Subject DNs ist gegeben, wenn niemals zwei oder mehr unterschiedliche Entitäten den gleichen Subject DN zugewiesen bekommen. |
| ISIS-MTT | Industrial Signature Interoperability Specification – MailTrust |
| ISO | International Organization for Standardization |
| LDAP | Lightweight Directory Access Protocol |
| OCSP | Online Certificate Status Protocol |
| PKI | Public Key Infrastruktur |
| PDS | PKI Disclosure Statement |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| URL | Uniform Resource Locator |
| ZDA | Zertifizierungsdiensteanbieter |

Glossar:

| | |
|------------------------------------|--|
| Authentifizierung | Die Authentifizierung (auch <i>Authentifikation</i> , engl. <i>authentication</i>) bezeichnet den Vorgang, die Identität einer Person oder eines Programms an Hand eines bestimmten Merkmals zu überprüfen. Dies kann zum Beispiel mit einem Fingerabdruck, einem Passwort oder einem beliebigen anderen Berechtigungsnachweis geschehen. Nah verwandt mit der Authentifizierung ist die Authentisierung . Die Authentisierung ist das Nachweisen einer Identität, die Authentifizierung deren Überprüfung. Im Englischen wird zwischen den beiden Begriffen nicht unterschieden, das Wort <i>authentication</i> steht für beides. |
| Authentisierung | Benutzer-Authentisierung Benutzer authentisiert sich zertifikatsbasiert gegenüber einer Anwendung mit seinem PSE, anstatt mit Kennung und Passwort. |
| Besitzer, Schlüsselbesitzer | Besitzer, Schlüsselbesitzer: Der Besitzer eines Schlüssels ist der End-User, der über den privaten Schlüssel berechtigterweise verfügt und für den korrekten Einsatz verantwortlich ist. |
| Certification Authority, CA | Certification Authority Instanz, die die Bindung eines Public Key's an einen Benutzer in Form eines Zertifikates herstellt und mit der eigenen digitalen Signatur beglaubigt. |
| Eigentümer, Schlüsseleigentümer | Der Eigentümer eines Schlüsselpaars ist der End-Benutzer, der für die korrekte Nutzung und Unversehrtheit des privaten Schlüssels verantwortlich ist. Der Eigentümer oder der Aussteller (CA) führt auch den Widerruf des Schlüsselpaars durch. |

| | |
|---|---|
| Identifizierung | Eine Identifizierung ist der Vorgang, der zum eindeutigen Erkennen einer Person oder eines Objektes dient. |
| LDAP | Lightweight Directory Access Protocol LDAP ist ein TCP/IP-basiertes Directory-Zugangsprotokoll, das sich im Internet und in Intranets als Standardlösung für sichere Verzeichnisdienste etabliert hat. |
| Nutzer, kryptographischer Verfahren in der PKI Öffentlicher Schlüssel, public key | Zertifikatsnutzer sind Personen, Organisationen, Maschinen, etc., die Zertifikate benutzen können um z.B. Verschlüsselungen durchzuführen, oder Signaturen zu prüfen. Der öffentliche Schlüssel ist der für jedermann zugängliche Teil eines Schlüsselpaars, das in der asymmetrischen Kryptographie verwendet wird. |
| Persönlicher Schlüssel | Ein asymmetrisches Schlüsselpaar ist ein persönliches Schlüsselpaar, wenn Besitzer und Eigentümer des dazugehörigen Personal Security Environments nur ein und dieselbe Person sein dürfen und der Name dieser Person im Zertifikat beglaubigt ist. |
| Persönlicher/ privater Schlüssel (private key) | Der private Schlüssel ist der geheime Teil des Schlüsselpaars (eines persönlichen Schlüssels, eines Funktionsschlüssels), der in der asymmetrischen Kryptographie verwendet wird. |
| Policy, PKI- | Ein Sicherheitskonzept besteht aus organisatorischen und technischen Maßnahmen und ist im Allgemeinen in einer Security-Policy niedergelegt. Die Public Key Infrastruktur wird in einer PKI-Policy niedergelegt und beschreibt das organisatorische Regelwerk, die technischen Komponenten sowie ihr Zusammenspiel. Die PKI-Policy ist das zentrale Dokument einer PKI schlechthin und definiert das Sicherheitslevel der PKI. Dieses Dokument beschreibt den Umgang mit Schlüsselmaterial unabhängig, wie es generiert oder zertifiziert/beglaubigt wurde und gilt für alle Teilnehmer am Verfahren. |
| Private Key | Beim symmetrischen Verfahren spricht man von einem geheimen Schlüssel, den beide Kommunikationspartner besitzen. Beim asymmetrischen Verfahren hat jeder Teilnehmer einen öffentlichen Schlüssel (Public Key) und einen privaten Schlüssel. Mit dem privaten Schlüssel wird signiert und mit dem öffentlichen Schlüssel die Unterschrift geprüft (validiert). Mit dem privaten Schlüssel kann der Empfänger die mit dem öffentlichen Schlüssel verschlüsselte Nachricht wieder entschlüsseln siehe auch Public Key Kryptographie |
| Public Key Infrastructure (PKI) | PKI ist die Summe aller Instanzen und Verfahren, die zum Einsatz der Public Key Kryptographie notwendig sind. Sie werden im Allgemeinen in einer Policy beschrieben. |
| Public Key Kryptographie | Verschlüsselungsverfahren, bei dem 2 verschiedene Schlüssel zum Ver- und zum Entschlüsseln einer Nachricht verwendet werden (daher auch die Bezeichnung asymmetrische Kryptographie). In der praktischen Anwendung wird einer dieser Schlüssel mit den Identifikationsdaten des Inhabers veröffentlicht (= public key) und der andere dem Inhaber auf einem sicheren Weg (häufig auf einer SmartCard) übergeben oder gleich in der SmartCard generiert. Eine wichtige Anwendung der Public Key Kryptographie ist die elektronische Signatur, bei der ein Dokument mit dem private key signiert wird und bei der dann der Empfänger mit Hilfe des public key |

| | |
|---|--|
| | die Signatur überprüft. |
| Registration Authority (RA) | Registration Authority, auch Local Registration Authority (LRA) Stelle, an der die zweifelsfreie Identitätsfeststellung des Endanwenders und die Ausgabe von Schlüsselmaterial stattfindet. |
| Registrierung | Feststellung der Identität im Personalisierungsprozess in einer (L)RA und signierte Weitergabe der Daten über einen sicheren Kanal an das Trustcenter. Voraussetzung ist die Antragstellung. Dem Teilnehmer im Verfahren für digitale Signaturen wird dabei ein geeigneter, eindeutiger Name zugewiesen. |
| S/MIME | Secure Multipurpose Internet Mail Extensions Ermöglicht das sichere Versenden und den sicheren Empfang von E-Mails. |
| Security Policy | Verbindliches Dokument zur Beschreibung der Sicherheitspolitik eines Unternehmens. Mögliche Geschäftsrisiken werden bewertet und ggf. Maßnahmen festgelegt. Risiken sind sowohl unerwartete negative Ereignisse als auch unrealisierte geschäftliche Chancen. IT-Security ist Teil der Sicherheitspolitik; PKI-Policy ist Teil der Security Policy. Somit ergänzt dieses Dokument die Security Policy des Einzelunternehmens. |
| Trust Center, Trustcenter Zertifizierungsdienst enabierter CSP (Certification Service Provider Verifizieren, Verifikation, Validierung | Instanz mit den möglichen Aufgaben Erzeugung von Schlüsselpaaren, sichere Aufbewahrung von Schlüsselmaterial, Ausstellen, Veröffentlichung und Rücknahme von Public Key-Zertifikaten, siehe auch Certification Authority, CA. |
| Verschlüsselung | Beim Verifizieren einer digitalen Signatur wird festgestellt, ob die signierten Daten unverfälscht sind und von der Person, Organisation, dem Verfahren oder der Einrichtung stammen, welche die digitale Signatur erstellt hat, siehe auch Hashwert. Die Verschlüsselung verhindert, dass unberechtigte Personen oder Dritte die elektronische Kommunikation verwerten können. Dabei werden mathematische Verfahren verwandt, welche die Daten in eine zwar lesbare, aber unverwertbare Form umwandeln (verschlüsseln). Die Rückumwandlung in die ursprüngliche Form (Entschlüsselung) ist nur autorisierten Personen, Organisationen, Verfahren oder Einrichtungen vorbehalten. |
| Widerruf, Revocation | Zertifikate können oder müssen in bestimmten Fällen durch die Eigentümer oder Besitzer oder Dritte, die nicht dem Unternehmen angehören, widerrufen werden, bevor ihre Gültigkeit abläuft. Mögliche Gründe, die einen Widerruf erzwingen, sind Offenlegung des Personal Security Environments (PSE), Diebstahl oder Verlust des PSE bzw. alle Fälle, in denen der Missbrauch eines PSE vermutet werden muss. Durch einen Widerruf wird der Gebrauch dieses Zertifikats und des zugehörigen PSE dauerhaft unterbunden; denn eine nachfolgende Aufhebung des Widerrufs ist nicht möglich. |
| Zertifikatsnutzer, Relying Party, Empfänger, Verifizierer, Validierer | Dies sind Personen, Organisationen, Verfahren oder Einrichtungen, die das Zertifikat bzw. den darin enthaltenen öffentlichen Schlüssel zum Verschlüsseln (vor dem Senden von Daten) oder Verifizieren (nach Empfang von signierten Daten) benutzen. |