Zertifizierungsrichtlinie des Europäischen Patentamts

Version 2.1

Gültig ab: 1. Januar 2011

Europäisches Patentamt
Bayerstrasse 35
80335 München
Deutschland
Tel.: +31 70 340 4500
http://www.epo.org

Zertifizierungsrichtlinie des Europäischen Patentamts

Ausgabedatum: 16. Mai 2011

Herausgeber
Europäisches Patentamt (EPA)

Das EPA ist das ausführende Organ der Europäischen Patentorganisation und hat seinen Hauptsitz in: Erhardtstraße 27, 80469 München, Deutschland. Es wird durch seinen Präsidenten vertreten.

Kontaktadresse
Bei Fragen zu dieser Zertifizierungsrichtlinie des EPA wenden Sie sich bitte an: eBusiness-Nutzerunterstützung, European Patent Office, Bayerstrasse 35, 80335 München, Deutschland, e-mail: support@epo.org

Copyright

Logo

Haftungsausschluss
Dieses Dokument enthält Angaben zu einigen Dienstleistungen, die in begrenztem Umfang und auch nur für eine bestimmte Nutzergruppe zur Verfügung stehen. Es gelten die hier aufgeführten Haftungsbeschränkungen.

Eine Gewähr dafür, dass der in diesem Dokument wiedergegebene Wortlaut von Rechtsvorschriften mit dem offiziell angenommenen Text übereinstimmt, wird nicht übernommen. Verbindlich sind allein die vom EPA veröffentlichte gedruckte Ausgabe des Europäischen Patentübereinkommens (EPÜ) und seiner Bestandteile und gegebenenfalls die in der Papierausgabe des Amtsblatts des EPA veröffentlichten Änderungen.

Mit diesen Haftungsausschlussklauseln wird nicht bezweckt, die Haftung entgegen den einschlägigen Bestimmungen des EPÜ oder denjenigen nationalen Rechtsvorschriften einzuschränken, auf die das EPÜ und dieses Dokument verweisen.

Sonstiges
Die vorstehenden Erklärungen und Hinweise sind nicht als Verzicht der Europäischen Patentorganisation auf die ihr als internationale Organisation eingeräumten Privilegien und Immunitäten zu verstehen, die ihr insbesondere durch das Protokoll über die Vorrechte und Immunitäten der Europäischen Patentorganisation vom 5. Oktober 1973 zugestanden werden. Das EPA behält sich vor, die in diesem Dokument beschriebenen Dienste und Inhalte im Rahmen der bestehenden Rechtsvorschriften jederzeit ohne Vorankündigung ganz oder teilweise zu ändern.

Documentenkontrolle

Änderungshistorie

Version	Datum	Beschreibung
1.0	15. April 2005	Erstausgabe
1.1	14. Juli 2005	Abschnitt 4.4.4 geäandert
2.0	1. März 2008	Aktualisierung des Dokuments nach Änderung gewisser rechtlichen Bestimmungen in verbindung mit dem Inkrafttreten des EPÜ2000
2.1	16. Mai 2011	Aktualisierung des Dokuments nach Änderung gewisser rechtlichen Bestimmungen und organisatorische Veränderungen

INHALTSVERZEICHNIS

GLOSSAR

Antragsteller	Eine Person, die eine Smartcard mit Teilnehmerzertifikaten beantragt, um Zugang zu den sicheren Diensten des EPA zu erhalten. Nach Genehmigung durch das EPA gilt diese Person als Zertifikatnehmer.
Eindeutiger Name (Distinguished Name, DN)	[Anhang F] Der eindeutige Name eines Zertifikatinhabers oder -nehmers. Jede Entität in der PKI-Domain muss einen klar erkennbaren und nur für sie verwendeten eindeutigen Namen haben, der im Feld "Subject Name" des Zertifikats steht.
EPA	Europäisches Patentamt
Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS)	[RFC 2537] Eine Erklärung zur Vorgehensweise einer CA bei der Ausstellung von Zertifikaten.
Kompromittierung	[Anhang F]Unbefugte Weitergabe, Änderung, Auswechslung oder Verwendung von vertraulichen, in Klartext vorliegenden kryptografischen Schlüsseln oder von anderen kritischen Sicherheitsparametern.
Kryptografisches Modul	[Anhang F] Die Hardware, Software und Firmware, entweder einzeln betrachtet oder auch in Kombination, welche Verschlüsselungslogiken oder -verfahren einschließlich Verschlüsselungsalgorithmen implementiert und sich innerhalb der kryptografischen Boundary des Moduls befindet.
Low-Level-Zertifikat	[Anhang F] Ein digitales Zertifikat, welches der Anmelder beispielsweise bei der Registrierung des Clients zur Online-Einreichung oder von einer Zertifizierungsstelle erhalten hat und welches ihn ohne vorherige Überprüfung seiner Identität ausweist.
Objektkennung (Object Identifier)	[Anhang F] Eine Nummer in einem speziellen Format, die bei einer international anerkannten Standardisierungsorganisation registriert ist. Mit ihrer Hilfe kann und sollte die bei einer Organisation geführte Dokumentensammlung zu PKIrelevanten Richtlinien und Verfahrensweisen eindeutig gekennzeichnet werden.

Öffentlicher Schlüssel (Public Key)	[Anhang F] In der PKI-Technologie stellt der öffentliche Schlüssel den
	Teil eines Paars aus öffentlichem und privatem Schlüssel im Besitz eines Nutzers dar, der anderen in der Nutzergemeinde über ein Zertifikat mit öffentlichem Schlüssel zugänglich gemacht wird. Mit dem öffentlichen Schlüssel eines Nutzers können andere Personen Daten für diesen Nutzer verschlüsseln und die digitale Signatur des Nutzers überprüfen.
PKI-Domain (Public Key Infrastructure Domain)	[Anhang F] Eine unabhängige Entität bestehend aus einer oder mehreren Zertifizierungsstellen, wo Zertifikatnehmer über das gleiche Selbst-oder Wurzelzertifikat verfügen.
Privater Schlüssel (Private Key)	[Anhang F] In der PKI-Technologie stellt der private Schlüssel den Teil eines Paars aus öffentlichem und privatem Schlüssel im Besitz eines Nutzers dar, der nur diesem bekannt ist. Mit dem privaten Schlüssel des Nutzers werden Daten digital signiert und Daten, die mit dem öffentlichen Schlüssel des Nutzers verschlüsselt wurden, wieder entschlüsselt.
Registrierungsstelle (Registration Authority, RA)	[Anhang F] Eine Entität, die für die Identifizierung und Authentifizierung von Zertifikatnehmern zuständig ist, nicht aber für die Signatur oder Ausstellung von Zertifikaten (d. h. eine Registrierungsstelle erhält von einer CA gewisse Aufgaben im Hinblick auf die Identitätsüberprüfung). Die RA kann Funktionen und entsprechende Vollmachten an lokale Registrierungsstellen delegieren.
Smartcard	Datenträger für private Teilnehmerschlüssel und Teilnehmerzertifikate
Sperrliste (Certificate Revocation List, CRL)	[Anhang F] Eine mit einem Zeitstempel versehene Liste mit gesperrten Zertifikaten, welche von einer CA digital signiert wurde.
Sperrung eines Zertifikats (Revocation)	[Anhang F] Vorzeitige Aufhebung der Gültigkeit eines Zertifikats ab einem bestimmten Datum.
Verzeichnisdienst (Repository)	[Anhang F] Ein System für die Speicherung und den Abruf von Zertifikaten und sonstigen zertifikatbezogenen Daten.

Zertifikat	[Anhang F] Ein Zertifikat verknüpft den Namen einer Entität (sowie weitere Attribute) mit dem jeweiligen öffentlichen Schlüssel. Ein Zertifikat muss der ITU-Empfehlung X.509, Version 3 entsprechen und muss auf jeden Fall • einen öffentlichen Schlüssel als Gegenstück zu einem privaten Schlüssel enthalten, über den allein sein Inhaber verfügt, • den Inhaber nennen oder anderweitig Aufschluss über ihn geben, • Aufschluss über die ausstellende Zertifizierungsstelle geben, • Angaben zur Gültigkeitsdauer enthalten, • die Seriennummer des Zertifikats enthalten, • die E-Mail-Adressen der End-Entitäten enthalten, • die digitale Signatur der ausstellenden Zertifizierungsstelle enthalten.
Zertifikatempfänger (Relying Party)	[RFC 2527] Der Empfänger eines Zertifikats, der im Vertrauen auf dieses Zertifikat und/oder auf digitale Signaturen handelt, die mit Hilfe dieses Zertifikats überprüft wurden.
Zertifikatnehmer (auch: Teilnehmer)	[Anhang F] Die natürliche Person, die in einem ihr ausgestellten Zertifikat namentlich erwähnt oder anderweitig ausgewiesen wird und die über einen privaten Schlüssel verfügt, der zu einem im Zertifikat aufgeführten öffentlichen Schlüssel gehört.
Zertifizierungsrichtlinie (Certificate Policy, CP)	RFC 2527] Ein anerkanntes Regelwerk, das die Anwendbarkeit eines Zertifikats auf eine bestimmte Gemeinschaft und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen festlegt. Eine Zertifizierungsrichtlinie kann beispielsweise die Anwendbarkeit eines bestimmten Zertifikattyps auf die Authentifizierung bei Vorgängen festlegen, die für den elektronischen Datenaustausch zum Warenhandel innerhalb eines bestimmten Preissegments erforderlich sind.
Zertifizierungsstelle (Certificate Authority, CA)	[Anhang F] Eine Zertifizierungsstelle ist eine vertrauenswürdige Instanz, die für eine Nutzergemeinschaft Zertifikate mit öffentlichem Schlüssel ausstellt und sperrt. Es ist Aufgabe der CA, die Informationen auf solchen Zertifikaten zu überprüfen. Unterstützt wird eine CA von CA-Servern, d. h. Computersystemen sowie von den Richtlinien und Verfahren rund um den Betrieb dieser Server. Der Ausdruck "Server" bezieht sich in diesem Fall auf die Hardware und Software zur eigentlichen Erzeugung von Zertifikaten und Zertifikat-Sperrlisten.

Abkürzungen

Anhang F	Anhang F, Anlage II zur PCT-PKI-Architektur für den e-PCT-Standard, gültig seit 1. Oktober 2005
CA	Zertifizierungsstelle (Certificate Authority)
CA für das EPA	Zertifizierungsstelle für das Europäische Patentamt
CN	Name (Certificate Common Name), Bestandteil des Distinguished Name
CP	Zertifizierungsrichtlinie (Certificate Policy)
CPS	Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement)
CRL	Sperrliste (Certificate Revocation List)
DN	Eindeutiger Zertifikatname (Certificate Distinguished Name)
EPA	Europäisches Patentamt
EPA-PKI	Public-Key-Infrastruktur des Europäischen Patentamts
EPÜ	Europäisches Patentübereinkommen
PCT	Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (Patent Cooperation Treaty)
PKI	Public-Key-Infrastruktur
RA	Registrierungsstelle (Registration Authority)
RA für das EPA	Registrierungsstelle für das Europäische Patentamt

Referenzen

In dieser Zertifizierungsrichtlinie des EPA wird auf folgende Dokumente Bezug genommen:

[Anhang F] WIPO, Patent Cooperation Treaty, Administrative Instructions under the Patent Cooperation Treaty: Modifications relating to the Electronic Filing and Processing of International Applications, Annex F, Appendix II -PKI Architecture for the e-PCT Standard, gültig seit 1. Oktober 2005

[RFC 2527] Network Working Group, Internet X.509 Public Key Infrastructure, Request for Comments: 2527, Certificate Policy and Certification Practices Framework, March 1999

[EPÜ] Übereinkommen über die Erteilung europäischer Patente (Europäisches Patentübereinkommen) vom 5. Oktober 1973, in der Fassung der Akte zur Revision von Art. 63 des Europäischen Patentübereinkommens vom 17. Dezember 1991 und der Akte zur Revision des Europäischen Patentübereinkommens vom 29. November 2000.

1. EINFÜHRUNG IN DIE ZERTIFIZIERUNGSRICHTLINIE DES EUROPÄISCHEN PATENTAMTS

1.1. Übersicht

1.1.1. Europäisches Patentamt und seine Online-Dienste

Das Europäische Patentamt (EPA) ist das ausführende Organ der Europäischen Patentorganisation. Es wurde durch das Europäische Patentübereinkommen (EPÜ) gegründet und ist mit verwaltungsmäßiger und finanzieller Selbständigkeit ausgestattet.

Nach einem einheitlichen und zentralisierten Verfahren erteilt es europäische Patente (Art. 4 EPÜ). Gemäß EPÜ, Teil X erfüllt das EPA ferner Aufgaben unter dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (Patent Cooperation Treaty, PCT).

Das EPA hat eine Palette von Online-Produkten und –Diensten entwickelt, damit Patentanmelder, Patentanwälte und andere Nutzer ihre Geschäfte mit dem EPA auf elektronischem Weg abwickeln können.

1.1.2. Sicherer Datenaustausch mit dem EPA

Eine Reihe dieser Produkte und Dienstleistungen stehen der breiten Öffentlichkeit ohne Registrierung zur Verfügung; zusätzlich ist aber auch eine geschützte Umgebung vorhanden, in der berechtigte Nutzer auf sicherem Weg Daten mit dem EPA austauschen können.

Im Normalfall handelt es sich bei berechtigten Nutzern um Anmelder oder Patentvertreter (zugelassene Vertreter, Mitarbeiter von Firmen mit Vertreterfunktion, Rechtsanwälte) (siehe Art. 133 und 134 EPÜ).

Um den Umgang mit den angebotenen geschützten Diensten zu vereinfachen, stellt das EPA berechtigten Nutzern seine Public-Key-Infrastruktur (EPA-PKI) zur Verfügung. Als Teil dieser Infrastruktur stellt die Zertifizierungsstelle (Certificate Authority) für das Europäische Patentamt (CA für das EPA) berechtigten Nutzern Teilnehmerzertifikate aus.

Dieses Dokument "Zertifizierungsrichtlinie des Europäischen Patentamts" (Certificate Policy, CP) beschreibt die Anforderungen im Hinblick auf Ausstellung, Verwendung und Sperrung von Teilnehmerzertifikaten innerhalb der EPA-PKI.

1.1.3. Sicherer Datenaustausch zwischen berechtigten Nutzern und anderen Institutionen zum Schutz des gewerblichen Eigentums

Ferner stellt das EPA im Rahmen bestimmter rechtlicher und sonstiger Vereinbarungen sicher, dass andere mit der Bearbeitung von Patentanmeldungen beauftragte nationale und internationale Organisationen und Institutionen und berechtigte Nutzer seine Online-Dienste ebenfalls zum oben genannten Zweck nutzen können.

Bei Erfüllung der jeweils geltenden Bedingungen und Erfordernisse kann die EPA-PKI daher auch Anmeldern, ihren Vertretern und anderen berechtigten Nutzern zur Verfügung gestellt werden, um ihnen den geschützten Datenaustausch mit anderen nationalen und internationalen Organisationen, die mit der Bearbeitung von Patentanmeldungen beauftragt sind, zu ermöglichen.

1.1.4. Allgemeine Beschreibung der EPA-PKI

Die EPA-PKI setzt sich zusammen aus:

- einer Zertifizierungsstelle (CA für das EPA), einschließlich eines Verzeichnisdienstes
- einer Registrierungsstelle (RA für das EPA)
- Zertifikatnehmern

Zertifikatnehmer sind berechtigte Nutzer gemäß Abschnitt 1.1.2 und 1.1.3. Teilnehmerzertifikate sind Zertifikate, die auf einer Smartcard an Anmelder, ihre Vertreter (Art. 134 (1), (8); 133 (3) EPÜ) sowie an jeden anderen Nutzer ausgegeben werden, der auf elektronischem Weg Daten mit dem EPA austauschen muss (siehe 1.1.1 oben).

Teilnehmerzertifikate werden nach Ermessen des EPA ausschließlich an natürliche Personen ausgegeben und gemäß Anhang F als "Low-Level-Zertifikate" definiert. Siehe auch Abschnitt 3 "Identifizierung und Authentifizierung" sowie Abschnitt 7 "Profil von Zertifikaten und Sperrlisten".

Auf Teilnehmerzertifikate sollten sich die jeweiligen Zertifikatempfänger (siehe unten) verlassen können.

1.1.5. Rechtsgrundlage für die EPA-PKI

Rechtsgrundlage für die elektronische Einreichung von europäischen Patentanmeldungen, internationalen (PCT-) Anmeldungen und sonstigen Unterlagen beim EPA und den zuständigen nationalen Behörden, sofern sie hierzu berechtigt sind, sind die Regel 2 EPÜ und Regel 89bis. 1 und 2 PCT.

Auf dieser Rechtsgrundlage werden in die Beschlüssen des Präsidenten des Europäischen Patentamts vom 12. Juli 2007, in denen es zum elektronischen Signaturen, Datenträger und Software (Sonderausgabe Nr. 3, Amtsblatt des EPA 2007, A5) geht, der Beschluss der Präsidentin des Europäischen Patentamts vom 26. Februar 2009 über die elektronische Einreichung von Unterlagendes (Amtsblatt des EPA 2009) und der Beschluss der Präsidentin des Europäischen Patentamts vom 8. Februar 2010 über die für die elektronische Einreichung von Unterlagen zu benutzende EPA-Software für die Online-Einreichung (Amtsblatt des EPA 2010, 226), Bedingungen für eine solche elektronische Einreichung genannt, zu denen auch die Verwendung elektronischer Signaturen gehört.

Die EPA-PKI erfüllt die Anforderungen in Bezug auf die elektronische Einreichung und Bearbeitung internationaler Anmeldungen, wie sie in Teil 7 und Anhang F der PCT-Verwaltungsrichtlinien dargelegt sind. Wo zutreffend, wurden Inhalt und Definitionen aus diesen Quellen in die Dokumente zur EPA-PKI übernommen.

Die Rechtsgrundlage für den elektronischen Datenaustausch des Zertifikatnehmers mit bestimmten anderen Beteiligten hängt von den geltenden Regeln und Bestimmungen für den Datenaustausch mit solchen Beteiligten ab und ist von diesen zu erfragen.

1.2. Kennzeichnung

Dieses Dokument trägt die Bezeichnung "Zertifizierungsrichtlinie des Europäischen Patentamts".
Eine eindeutige Dokumentenkennung (Object Identifier) wurde für dieses Dokument nicht vergeben.

1.3. Nutzergemeinde und Anwendbarkeit

Das EPA ist Zertifizierungsstelle und als solche Dienstleistungsanbieter für Zertifikatnehmer. Um diese Dienste anbieten zu können, unterhält das EPA die EPA-PKI, die aus mehreren technischen Komponenten besteht.

Dieser Abschnitt beschreibt die Komponenten der EPA-PKI sowie die Anwendbarkeit der innerhalb der EPA-PKI ausgestellten Zertifikate.

1.3.1. Zertifizierungsstellen

Zertifizierungsstelle (CA) innerhalb der EPA-PKI ist die CA für das Europäische Patentamt. Diese stellt alle Teilnehmerzertifikate aus.

Das Zertifikat der CA für das EPA selbst wurde von der Zertifizierungsstelle für die Europäische Patentorganisation zertifiziert. Diese Wurzel-Zertifizierungsstelle kann bei Bedarf Zertifikate für nachgeordnete Zertifizierungsstellen der Organisation ausstellen.

1.3.2. Registrierungsstelle für das EPA

Die RA für das EPA ist für die Identifizierung und Authentifizierung von Antragstellern innerhalb der EPA-PKI zuständig.

1.3.3. Zertifikatnehmer

Zertifikatnehmer sind natürliche Personen, welche die innerhalb der EPA-PKI erzeugten und auf einer Smartcard gespeicherten Zertifikate und privaten Schlüssel nutzen.

1.3.4. Zertifikatempfänger

1.3.4.1. EPA

Im Sinne der CP gilt das EPA als Zertifikatempfänger.

1.3.4.2. Anmeldeamt

Andere Entitäten können Zertifikatempfänger sein, sofern sie unter dem PCT (siehe Art. 10 PCT) als Anmeldeamt in Frage kommen, dem Internationalen Büro mitgeteilt haben (siehe Abschnitt 703 Verwaltungsvorschriften), dass sie zur Annahme internationaler Anmeldungen in elektronischer Form bereit sind, und u. a. erklären, dass sie im Hinblick auf die elektronische Signatur, die für die internationale Einreichung erforderlich ist (siehe Abschnitt 710 (a) unter (vi) Verwaltungsvorschriften), die CA für das EPA als Zertifikatausstellerin anerkennen.

Das Internationale Büro hat die vorstehend erwähnte Mitteilung zu veröffentlichen (siehe Abschnitt 710 (c) Verwaltungsvorschriften).
Die Berechtigung des Zertifikatempfängers, sich unter den vorstehenden Bedingungen auf die von der CA für das EPA ausgestellten Zertifikate verlassen zu können, ist auf die Vorgänge im PCT-Verfahren beschränkt, die eine elektronische Signatur erfordern. Soll die Berechtigung eines Zertifikatempfängers, sich auf Zertifikate verlassen zu können, erweitert werden, so ist hierfür eine über diesen Abschnitt hinausgehende Rechtsgrundlage erforderlich.

1.3.4.3. Zentralbehörde für den gewerblichen Rechtsschutz

Andere Entitäten können Zertifikatempfänger sein, sofern sie als zentrales Amt für

gewerbliches Eigentum eines EPÜ-Vertragsstaats oder aber eines Nichtvertragsstaats, der vom EPA als Zertifikatempfänger benannt wurde, handeln. Zu diesem Zweck kann das EPA gegebenenfalls Anforderungen und Bedingungen aufstellen, die vom betreffenden zentralen Amt für gewerbliches Eigentum zu erfüllen sind.

1.3.4.4. Regierungsorganisationen

Gewisse Entitäten, die als mit der Patenterteilung beauftragte Regierungsorganisationen handeln, können Zertifikatempfänger sein, sofern sie vom EPA als solche benannt wurden. Zu diesem Zweck kann das EPA gegebenenfalls Anforderungen und Bedingungen aufstellen, die von der betreffenden Regierungsorganisation zu erfüllen sind.

1.3.5. Anwendbarkeit

Die vom EPA herausgegebene Smartcard enthält zwei Arten von Teilnehmerzertifikaten: Authentifizierungszertifikate, mit denen sich der Zertifikatnehmer in einer Netzwerkumgebung ausweist, und Nachweisbarkeitszertifikate, mit denen er ein Dokument elektronisch signieren kann.

Teilnehmerzertifikate sind nur auf Dienste anwendbar, die vom EPA oder einem Zertifikatempfänger bereitgestellt werden.

1.4. Kontaktadressen

1.4.1. Verwaltung der Zertifizierungsrichtlinie

Die Zertifizierungsrichtlinie wird vom Direktorat Sicherheit und Audit des EPA gepflegt.

1.4.2. Kontaktadresse bei Anfragen

Dieses Dokument kann unter http://www.epo.org/applying/online-services/security/smart-cards_de.html heruntergeladen werden. Anfragen können Sie auch an folgende Adresse richten:
eBusiness-Nutzerunterstützung, European Patent Office, Bayerstrasse 35, 80335 München, Deutschland,
e-mail:support@epo.org

1.4.3. Überprüfung der Konformität von CPS und CP

Ob die vom EPA abgegebene Erklärung zum Zertifizierungsbetrieb (CPS) mit dieser Richtlinie in Einklang steht, ermittelt das in Abschnitt 1.4.1, Verwaltung der Zertifizierungsrichtlinie, genannte Gremium.

1.5. Inkrafttreten/Übergangsrecht

Die CP tritt an dem Tag in Kraft, der auf dem Deckblatt als Gültigkeitsdatum angegeben ist.

Das in der CP angegebene Ausgabedatum ist das Datum, an dem die aktuelle Version gemäß Abschnitt 2.6 zur Veröffentlichung freigegeben wurde.

Für den Fall, dass das Gültigkeitsdatum vor dem Ausgabedatum liegt, wird in diesem Abschnitt 1.5 bestätigt, dass für die EPA-PKI die Bedingungen der CP rückwirkend ab diesem Gültigkeitsdatum gelten.

Sofern in der CP nichts anderes vorgesehen ist, gilt immer deren letzte Version, also auch für alle vor dem Gültigkeitsdatum ausgestellten Zertifikate.

Im Hinblick auf den Betrieb der EPA-PKI gelten spätere Ausgaben der CP ab dem Datum, das auf dem revidierten Dokument angegeben ist.

Diese Bestimmungen gelten auch für alle anderen Dokumente im Zusammenhang mit der CP (und ihren späteren Versionen) wie beispielsweise CPS und Verpflichtungserklärungen von Zertifikatnehmern und Zertifikatempfängern.

2. ALLGEMEINE BESTIMMUNGEN

2.1. Verpflichtungen

2.1.1. Verpflichtungen der CA für das EPA

Die CA für das EPA erfüllt die Verpflichtungen, wie sie in der CP und/oder den hierauf basierenden Dokumenten einschließlich der CPS festgelegt sind. Die CA für das EPA hat u. a. folgende Verpflichtungen:

- Sie handelt im Einklang mit den Bestimmungen der CP und der zugehörigen CPS.
- Sie ergreift geeignete Maßnahmen, um zu gewährleisten, dass ihr eigener privater Schlüssel geheim bleibt, und stellt eine geschützte Umgebung für die Zugangs-und Nutzungskontrolle bereit.
- Sie ermöglicht berechtigten Nutzern der EPA-PKI den Zugriff auf die CP.
- Nach Eingang eines zulässigen Antrags von der RA für das EPA stellt sie dem Antragsteller den Bedingungen der CPS entsprechend ein Teilnehmerzertifikat aus.
- Nach Eingang eines zulässigen Sperrantrags sperrt sie den Bedingungen der CP entsprechend das betreffende Teilnehmerzertifikat und setzt den Zertifikatnehmer hiervon in Kenntnis.
- Sie spielt ausgestellte Teilnehmerzertifikate in den Verzeichnisdienst ein. (Anmerkung: Für den Zugriff auf diesen Verzeichnisdienst ist eine entsprechende Berechtigung erforderlich.)
- Sie erzeugt Teilnehmerschlüsselpaare auf der jeweiligen Smartcard, leitet die Zertifikatanträge zur Zertifizierung weiter, speichert das Teilnehmerzertifikat wieder auf der Smartcard ab und verschickt Smartcard und Smartcard-PIN an den Zertifikatnehmer.
- Sie erzeugt eine Sperrliste und veröffentlicht diese im Verzeichnisdienst.

2.1.2. Verpflichtungen der RA für das EPA

Die RA für das EPA erfüllt die Verpflichtungen, wie sie in der CP und/oder den hierauf basierenden Dokumenten einschließlich der CPS festgelegt sind. Die RA für das EPA hat u. a. folgende Verpflichtungen:

- Sie handelt im Einklang mit den Bestimmungen der CP und der zugehörigen CPS.
- Sie stellt die Zulässigkeit von Zertifikatanträgen sicher.
- Sie nimmt Anträge auf Ausstellung von Teilnehmerzertifikaten entgegen und bearbeitet diese.
- Sie nimmt von dazu berechtigten Personen (siehe Abschnitt 4.4.2) Sperranträge entgegen, prüft mit angemessenem Aufwand die Zulässigkeit dieser Anträge und leitet die für zulässig erklärten Anträge an die CA für das EPA weiter.
- Sie setzt Zertifikatnehmer und CA für das EPA von der Sperrung des Teilnehmerzertifikats in Kenntnis.

2.1.3. Verpflichtungen des Zertifikatnehmers

Der Zertifikatnehmer erfüllt die Verpflichtungen, wie sie in der CP und/oder den hierauf basierenden Dokumenten einschließlich der CPS und gegebenenfalls in der Verpflichtungserklärung des Zertifikatnehmers festgelegt sind. Der Zertifikatnehmer hat u. a. folgende Verpflichtungen:

- Er stellt sicher, dass öffentliche und private Schlüssel sowie Teilnehmerzertifikate nur den Bedingungen der CP entsprechend verwendet werden.
- Bei der Beantragung eines Zertifikats macht er richtige und vollständige Angaben.
- Er stellt sicher, dass der private Schlüssel sowie die PIN, welche die Smartcard mit dem privaten Schlüssel schützt, entsprechend den Bedingungen der CP stets gegen Verlust, Weitergabe an Unbefugte, Veränderung und unbefugte Nutzung geschützt sind.
- Er stellt sicher, dass nur er selbst Kenntnis von der Teilnehmer-PIN hat.
- Bei einer tatsächlichen oder mutmaßlichen Kompromittierung der privaten Schlüssel, der PIN oder der Smartcard oder bei Änderung von Angaben im Zertifikatantrag reicht er bei der RA für das EPA unverzüglich einen Sperrantrag ein.

2.1.4. Verpflichtungen des Zertifikatempfängers

Der Zertifikatempfänger erfüllt die Verpflichtungen, wie sie in der CP und/oder den hierauf basierenden Dokumenten einschließlich der CPS und gegebenenfalls in einer Verpflichtungserklärung des Zertifikatempfängers festgelegt sind. Der Zertifikatempfänger hat u. a. folgende Verpflichtungen:

- Er überprüft selbstständig die Zweckdienlichkeit eines Zertifikats sowie dessen tatsächliche Nutzung für den vorbestimmten Zweck.
- Vor der Verifizierung eines vorgelegten Zertifikats überprüft er dieses auf Sperrung oder Aussetzung.

2.2. Haftung

2.2.1. Umfang der vom EPA zu übernehmenden Haftung

2.2.1.1.

Durch den Betrieb der EPA-PKI und insbesondere durch die Signierung eines Zertifikats, welches die Anwendung der Zertifizierungsrichtlinien (CP) bestätigt, stellt das EPA gegenüber denjenigen, die auf die Angaben in diesem Zertifikat angemessen vertrauen (siehe 1.3.4), lediglich sicher, dass der Zertifizierungs-und Verzeichnisdienstbetrieb, die Ausstellung und Sperrung von Zertifikaten sowie die Herausgabe von CRLs der CP entsprechend erfolgen. Die Verpflichtung des EPA beschränkt sich auf die Ergreifung geeigneter Maßnahmen, um sicherzustellen, dass Zertifikatnehmer und Zertifikatempfänger beim Umgang mit Zertifikaten, die einen Verweis auf die CP oder die entsprechenden Schlüssel enthalten, die CP beachten (siehe 2.2.4).

2.2.1.2.

Das EPA haftet nicht für die Folgen, wenn CP-konform ausgestellte Zertifikate für einen anderen Zweck als den Datenaustausch zwischen EPA und berechtigten Nutzern verwendet werden (siehe 1.1.2 und 1.3.4.1). Das EPA haftet nicht für die Verwendung von CP-konform ausgestellten Zertifikaten, die für den Datenaustausch zwischen berechtigten Nutzern und anderen Einrichtungen für gewerbliches Eigentum oder Dritten genutzt werden (siehe 1.1.3 und 1.3.4.2 / 1.3.4.3 / 1.3.4.4). Dies steht einer eventuellen Haftung von Zertifikatempfängern gegenüber den jeweiligen Zertifikatnehmern nicht entgegen.

2.2.2. Haftungsbeschränkung

2.2.2.1.

Die Verfügbarkeit der EPA-PKI kann durch Wartungs-und Reparaturarbeiten am System oder durch Faktoren, die sich der Einflussnahme des EPA entziehen, beeinträchtigt sein. Für die Nichtverfügbarkeit der EPA-PKI übernimmt das EPA daher keine Haftung.

2.2.2.2.

Eine Haftung für Schäden ist ausgeschlossen, es sei denn, dass das EPA den Schaden vorsätzlich oder durch grobe Fahrlässigkeit verursacht hat oder dass der Schaden Leben und Gesundheit betrifft oder dass die nicht eingehaltene Verpflichtung grundsätzlicher Natur ist. Handelt es sich im letztgenannten Fall bei dem Ansprucherhebenden nicht um einen Verbraucher (im Sinne von Art. 13 Bürgerliches Gesetzbuch), beschränkt sich die Haftung des EPA auf den typischerweise vorhersehbaren Schaden.

2.2.3. Maßgebliches Recht für die Haftung des EPA

Unbeschadet der Bestimmung zum maßgeblichen Recht (siehe Abschnitt 2.4.1) bestimmt sich die Haftung des EPA nach Art. 9 EPÜ. Im Hinblick auf die Anwendung von Art. 9 (1) und (2) EPÜ ist das deutsche Recht maßgeblich.

2.2.4. Haftung von Zertifikatnehmer und Zertifikatempfänger

Verpflichtungserklärungen von Zertifikatnehmern und Zertifikatempfängern spiegeln die beschränkte Haftung des EPA wider (siehe Abschnitt 2.2), und in diesen Erklärungen haben Zertifikatnehmer/Zertifikatempfänger gegebenenfalls die Einhaltung der in Abschnitt 2.1.3 bzw. 2.1.4 aufgelisteten Verpflichtungen zu garantieren.

2.3. Finanzielle Verantwortung

2.3.1. Entschädigung durch Zertifikatempfänger

Soweit unter dem maßgeblichen Recht zulässig, enthalten Verpflichtungserklärungen von Zertifikatnehmern/Zertifikatempfängern die Bestimmung, dass diese das EPA für alle Folgen zu entschädigen haben, die sich aus der Nichteinhaltung der Bedingungen in solchen Verpflichtungserklärungen oder an anderer Stelle in der EPA-PKI-Dokumentation ergeben.

2.3.2. Vertreterfunktionen

Die Ausstellung von Zertifikaten durch die CA für das EPA bedeutet nicht, dass diese für Zertifikatnehmer oder Zertifikatempfänger die Funktion eines Bevollmächtigten, Treuhänders oder irgendeines anderen Vertreters übernimmt.

2.3.3. Verwaltung

Keine Angaben

2.4. Auslegung und Durchsetzung

2.4.1. Maßgebliches Recht

2.4.1.1. Maßgebliches Recht

Das maßgebliche Recht bestimmt sich nach dem Europäischen Patentübereinkommen und den darauf aufbauenden Regeln und Bestimmungen. Der PCT sowie die darauf aufbauenden Regeln und sonstigen Vorschriften sind gemäß EPÜ oder CP anzuwenden.

Daneben gilt das deutsche Recht, wobei der Rückgriff auf das deutsche Streitregelungsrecht ausgeschlossen ist.

Diese Bestimmung zum maßgeblichen Recht gilt für die CP und sonstige Dokumente, die sich auf die CP-basierte EPA-PKI beziehen, wie beispielsweise die CPS oder Verpflichtungserklärungen von Zertifikatnehmern und Zertifikatempfängern, sofern in solchen Dokumenten nichts anderes angegeben ist.

Diese Bestimmung zum maßgeblichen Recht steht der Anwendbarkeit anderen nationalen Rechts im Verhältnis von Zertifikatempfängern einerseits und Zertifikatnehmern andererseits nicht entgegen. Für das EPA gilt der letzte Satz nicht.

Diese Bestimmung zum maßgeblichen Recht geht von dem Grundsatz aus, dass für alle in der EPA-PKI Beteiligten unabhängig von ihrem Standort einheitliche Verfahren und eine einheitliche Auslegung sicherzustellen sind.

2.4.1.2. Vorrechte und Immunitäten der Europäischen Patentorganisation

Die CP ist so auszulegen, dass die im EPÜ beschriebenen Rechte der Europäischen Patentorganisation einschließlich des Protokolls über Vorrechte und Immunitäten der Europäischen Patentorganisation vom 5. Oktober 1973 in allen Fällen gewahrt bleiben.

2.4.2. Sonstiges

Sollten eine oder mehrere Bestimmungen der CP aus irgendeinem Grund für unzulässig, ungesetzlich oder rechtlich nicht durchsetzbar erklärt werden, so hat dies keinerlei Auswirkungen auf andere Bestimmungen, sondern die CP ist dann so lesen, als ob diese nicht durchsetzbare(n) Bestimmung(en) nicht darin enthalten wären; sie sollte möglichst in ihrem ursprünglichen Sinn ausgelegt werden.

Keine der in der CP enthaltenen Bedingungen und Bestimmungen darf geändert, fallen gelassen, ergänzt, modifiziert oder aufgehoben werden, es sei denn, dies erfolgt im Einklang mit den in der CP festgeschriebenen Verfahren.

Benachrichtigungen, Genehmigungen, Anträge und sonstige Mitteilungen, welche die CA für das EPA entsprechend der CP verfasst, werden elektronisch oder in Papierform versandt.

2.4.3. Streitregelungsverfahren

Bei Streitfällen im Zusammenhang mit dem Betrieb der EPA-PKI, der CP, der CPS oder anderen Dokumenten mit Bezug auf die EPA-PKI bemühen sich die Beteiligten um eine gütliche Beilegung im Verhandlungsweg.

Streitigkeiten, die sich aus oder im Zusammenhang mit dem Betrieb der EPA-PKI ergeben und an denen das EPA als Partei beteiligt ist, werden gemäß Zivilprozessordnung (ZPO) durch den bindenden Schiedsspruch nur eines Schiedsrichters beigelegt. Das Schiedsverfahren findet in München statt.

Wenn das EPA jedoch auf seine Immunität von der nationalen Gerichtsbarkeit verzichtet, obliegt bei solchen Streitigkeiten die Rechtsprechung den Gerichten in München.

Tritt während des Betriebs der EPA-PKI ein Ereignis ein, für das eine der Parteien nach geltendem Patentrecht eine Regelung verlangen kann, so haben die dort festgelegten

Rechtsinstrumente Vorrang vor den vorstehend genannten Streitregelungsverfahren. Es gelten die Bestimmungen in Abschnitt 2.4.1.2.

Verpflichtungserklärungen von Zertifikatnehmern und Zertifikatempfängern enthalten eine Streitregelungsklausel mit den vorstehend genannten Grundsätzen, sofern bestimmte Umstände nicht andere Festlegungen erfordern.

2.5. Gebühren

Die von Zertifikatnehmern und Zertifikatempfängern zu entrichtenden Gebühren für die Nutzung der EPA-PKI, für die Zertifikatverwaltung, für die Nutzung von Smartcard und anderen in der CP oder CPS genannten Komponenten oder Diensten sind in den Gebühren für die Dienstleistungen des EPA enthalten oder aber getrennt ausgewiesen.

2.5.1. Gebühren für die Ausstellung oder Erneuerung von Zertifikaten

Smartcards, Zertifikate und Unterstützungsprogramme werden dem Zertifikatnehmer im Normalfall kostenlos zur Verfügung gestellt. Das EPA behält sich allerdings das Recht vor, unter gewissen Umständen eine Gebühr zu erheben.

2.5.2. Gebühren für die Bereitstellung von Zertifikaten

Für die Bereitstellung von Zertifikaten für Zertifikatempfänger erhebt das EPA im Normalfall keine Gebühren.

2.5.3. Gebühren für die Bereitstellung von Sperr-oder Statusinformationen

Informationen zur Sperrung werden kostenlos bereitgestellt.

2.5.4. Gebühren für sonstige Dienste wie Auskunft über Zertifizierungsrichtlinien

Für die Bereitstellung von Informationen über Zertifizierungsrichtlinien, wie sie z. B. in der CP und der CPS enthalten sind, erhebt das EPA keine Gebühren.

2.5.5. Rückerstattungen

Keine Angaben

2.6. Veröffentlichung und Verzeichnisdienst

2.6.1. Veröffentlichung von Daten der CA für das EPA

Das EPA veröffentlicht folgende Daten aus dem Verzeichnisdienst (zumindest auf einer Website im Internet):

- Zertifizierungsrichtlinie des EPA
- Erklärung zum Zertifizierungsbetrieb des EPA
- Zertifikat der CA für die Europäische Patentorganisation (Wurzelzertifikat)
- Verpflichtungserklärung von Zertifikatnehmern
- Verpflichtungserklärung von Zertifikatempfängern
- Zertifikat der CA für das EPA
- Verzeichnis der Sperrlisten

2.6.2. Häufigkeit der Veröffentlichung

Die CA für das EPA veröffentlicht die in Abschnitt 2.6.1 genannten Daten, sobald sie ihr vorliegen.

2.6.3. Zugriffskontrolle

Die CA für das EPA kontrolliert den Zugriff auf ihren Verzeichnisdienst, um die

Aktualisierung oder Löschung der darin gespeicherten Daten durch Dritte zu verhindern.

2.6.4. Verzeichnisdienste

Im Hinblick auf die Veröffentlichung von Teilnehmerzertifikaten und CRLs unterhält die CA für das EPA einen Verzeichnisdienst.

2.7. Konformitätsprüfung

2.7.1. Häufigkeit der Konformitätsprüfung auf Entitätsebene

Um zu prüfen, ob die in der CPS aufgeführten Sicherheitsmechanismen angewandt werden, führt das EPA regelmäßige und Ad-hoc-Kontrollen seiner Betriebsräume und Geschäftsvorgänge durch. Ferner beauftragt es einen unabhängigen externen Prüfer mit der Durchführung einer Jahresprüfung.

2.7.2. Identität/Qualifikationen des Prüfers

Ein unabhängiger externer Prüfer führt einmal jährlich eine Prüfung durch. Der Prüfer ist Mitarbeiter eines kompetenten professionellen Unternehmens, das sich an die einschlägigen nationalen und internationalen Grundsätze und Verhaltensregeln hält.

2.7.3. Verhältnis Prüfer/geprüfte Instanz

Die Durchführung der Prüfung und Vorlage des Berichts werden durch einen Vertrag zwischen Prüfer und geprüfter Instanz geregelt.

2.7.4. Gegenstand der Prüfung

In der Prüfung wird ermittelt, ob die EPA-PKI-Systeme und -Verfahren mit CP und CPS des EPA in Einklang stehen. Ferner wird unter Bezug auf die vorgegebenen Prüfungsziele ermittelt, welche Geschäftsrisiken sich aus der Nichterfüllung von CP und CPS ergeben.

2.7.5. Maßnahmen zur Mängelbeseitigung

Hat die Prüfung Mängel ergeben, so ergreift das EPA die seiner Einschätzung nach notwendigen und angemessenen Maßnahmen, um diese zu beseitigen.

2.7.6. Bekanntgabe von Ergebnissen

Der Betrieb der EPA-PKI unter Einhaltung der entsprechenden Bedingungen und Vorschriften obliegt dem EPA. Der detaillierte Prüfungsbericht wird nur dem EPA bekannt gemacht.

2.8. Vertraulichkeit

2.8.1. Vertraulich zu behandelnde Daten

- Das EPA schützt den Inhalt von Anträgen auf Ausstellung oder Sperrung eines Zertifikats unabhängig von deren Erfolg als vertrauliche Daten, die nur der CA für das EPA und dem Antragsteller bekannt sind. In den unter 2.8.2 bis 2.8.7 genannten Fällen gilt dies jedoch nicht.
- Einzelheiten zu Sicherheit und Geschäftsvorgängen behandelt das EPA als vertrauliche Informationen, die sonst nur dem jeweiligen Zertifikatnehmer und Zertifikatempfänger bekannt sind. Auf Anfrage hat das EPA diese Informationen allerdings dem beauftragten Prüfer zu offenbaren.

2.8.2. Nicht vertrauliche Daten

Daten in Zertifikaten, Sperrlisten oder der CP sieht das EPA als nicht vertraulich an.

2.8.3. Offenlegung von Daten zur Sperrung/Aussetzung von Zertifikaten

Der Inhalt von Sperrlisten sowie der Status einzelner Zertifikate wird den jeweiligen Zertifikatempfängern vorbehaltlos offenbart.

2.8.4. Offenlegung gegenüber Strafverfolgungsbehörden

Das EPA ist berechtigt, Daten, über die es in seiner Funktion als CA oder RA oder in Verbindung mit dem Betrieb der EPA-PKI verfügt, offen zu legen, soweit eine solche Offenlegung unter dem für die CP maßgeblichen Recht zulässig ist und ihr ein nachprüfbares und geeignetes Rechtsinstrument (wie z. B. eine richterliche Verfügung) zugrunde liegt. Dies gilt unbeschadet der Vorrechte und Immunitäten des EPA.

2.8.5. Offenlegung in Zivilverfahren

Das EPA ist berechtigt, vertrauliche Daten über einen bestimmten Zertifikatnehmer in einem Zivilverfahren offen zu legen, soweit eine solche Offenlegung unter dem für die CP maßgeblichen Recht zulässig ist und ihr ein nachprüfbares und geeignetes Rechtsinstrument zugrunde liegt. Dies gilt unbeschadet der Vorrechte und Immunitäten des EPA.

2.8.6. Offenlegung auf Antrag des Zertifikatnehmers

Das EPA offenbart einem Zertifikatnehmer auf Antrag alle vertraulichen Daten, die über ihn vorliegen.

2.8.7. Sonstige Fälle von Offenlegung

Keine Angaben

2.9. Geistige Eigentumsrechte

Alle geistigen Eigentumsrechte an Teilnehmerzertifikaten und der CP sind und bleiben Eigentum des EPA.

3. IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1. Erstregistrierung

3.1.1. Namen

Zum Nachweis der Identität verwendet die CA für das EPA sowohl für sich selbst als auch für Zertifikatnehmer eindeutige Namen (Distinguished Name, DN) mit den für eindeutige Namen festgelegten Attributen gemäß Standard ITU-T X.501.

3.1.2. Aussagekraft von Namen

Die CA für das EPA stellt sicher, dass ein Attributsatz einen Zertifikatnehmer eindeutig identifiziert und aussagekräftige Werte enthält.

3.1.3. Regeln zur Auslegung verschiedener Namensformen

Keine Angaben

3.1.4. Eindeutigkeit von Namen

Die CA für das EPA vergibt eindeutige Namen gemäß 3.1.1 und 3.1.2. Zertifikatanträge, bei denen der Name des Antragstellers nicht hinreichend vom Namen eines anderen Zertifikatnehmers zu unterscheiden ist, lehnt die CA für das EPA ab.

3.1.5. Streitregelungsverfahren bei Beanspruchung des gleichen Namens

Mögliche Streitigkeiten über die Namensvergabe versucht die CA für das EPA zu lösen, indem sie Kontakt mit dem Antragsteller aufnimmt und sich beispielsweise zur Änderung des Attributs CN (Common Name) bereit erklärt, um die Eindeutigkeit des DN herzustellen.

3.1.6. Erkennung, Authentifizierung und Rolle von Marken

Die CA für das EPA ist nicht verpflichtet, nach Hinweisen auf die Verletzung von Markenrechten zu suchen.

3.1.7. Nachweis für den Besitz eines privaten Schlüssels

Nicht zutreffend, da Teilnehmerschlüssel von der CA für das EPA erzeugt werden.

3.1.8. Authentifizierung der Identität von Organisationen

Die CA für das EPA legt in ihrer CPS fest, wie die Identität einer Organisation zu authentifizieren ist.

3.1.9. Authentifizierung der Identität von Einzelpersonen

Bevor ein Antragsteller ein Zertifikat erhält, wird seine Identität von der RA für das EPA nach dem Registrierungsverfahren authentifiziert. Die RA für das EPA ergreift alle geeigneten Maßnahmen, um die Identität des Antragstellers zu überprüfen.

3.2. Zertifikaterneuerung im Normalfall

Solange ihr Zertifikat gültig ist, weisen sich Zertifikatnehmer mit ihrer Smartcard aus. Zur Erneuerung abgelaufener Zertifikate ist wie bei der Erstregistrierung zu verfahren.

3.3. Zertifikaterneuerung nach Sperrung

Zur Erneuerung gesperrter Zertifikate ist im Hinblick auf Identifizierung und Authentifizierung wie bei der Erstregistrierung zu verfahren.

3.4. Antrag auf Sperrung

In ihrer CPS macht die CA für das EPA genaue Angaben zu Identifizierungs-und Authentifizierungsverfahren und Maßnahmen, die zur Authentifizierung von Sperranträgen erforderlich sind,

4. BETRIEBSANFORDERUNGEN

4.1. Antrag auf Ausstellung eines Zertifikats

Bei jedem Antrag auf Ausstellung eines Zertifikats führt der Antragsteller folgende Schritte aus:

- Er weist sich gemäß Abschnitt 3 gegenüber der RA für das EPA aus.
- Er beantragt einen (neuen) privaten Schlüssel, der im Einklang mit dieser Richtlinie erzeugt und geschützt wird, oder aber er legt einen öffentlichen Schlüssel vor und weist nach, dass er im Besitz des entsprechenden privaten Schlüssels ist und dass dieser im Einklang mit dieser Richtlinie erzeugt und geschützt wurde.
- Er übermittelt persönliche Daten, die zusammen mit dem Antrag zertifiziert und/oder gespeichert werden.

CA für das EPA und RA für das EPA gehen bei der Annahme und Bearbeitung von Zertifikatanträgen mit der gebotenen Sorgfalt vor. Die CA für das EPA dokumentiert die Verfahren zur Bearbeitung von Zertifikatanträgen in allen Einzelheiten.

4.2. Ausstellung von Zertifikaten

In dem Augenblick, wo die CA für das EPA ein Zertifikat ausstellt, gilt der Zertifikatantrag als vollumfänglich und unwiderruflich genehmigt.

Das Verfahren zur Erzeugung von Zertifikaten und den entsprechenden privaten Schlüsseln und Tokens gliedert sich in fünf deutliche unterscheidbare Teile (oder Funktionen) mit ihren jeweiligen Untersystemen.

Dabei handelt es sich um folgende Funktionen:

1 Erzeugung von Schlüsseln
2 Speicherung im Token
3 Erzeugung von Zertifikaten
4 Erzeugung von PINs
5 Verteilung und Auslieferung

4.3. Abnahme von Zertifikaten

Der Zertifikatnehmer bestätigt den Erhalt seiner Smartcard und damit die Abnahme des Zertifikats.

4.4. Sperrung von Zertifikaten

Zertifikate, die ihre Gültigkeit oder Vertrauenswürdigkeit verloren haben, werden gesperrt.

4.4.1. Bedingungen für die Sperrung

Die Sperrung eines Zertifikats kann vom Zertifikatnehmer beantragt werden. Gründe für die Sperrung eines Zertifikats sind beispielsweise:

- Diebstahl, Verlust, Weitergabe an Dritte, Änderung oder sonstige Kompromittierung oder mutmaßliche Kompromittierung des privaten Schlüssels des Zertifikatnehmers, seiner PIN oder seiner Smartcard
- Vorsätzlicher Missbrauch von Schlüsseln und/oder Zertifikaten durch den Zertifikatnehmer

- Erhebliche Missachtung der Erfordernisse hinsichtlich des Zertifizierungsbetriebs, wie sie in der CP oder anderen relevanten Dokumenten (z. B. Verpflichtungserklärung des Zertifikatnehmers) festgelegt sind
- Falsche Angaben im Zertifikat, die nachträglich oder aufgrund neuer Entwicklungen festgestellt wurden
- Unzulässige Ausstellung (z. B. bei falschen Angaben im Zertifikat) oder fehlerhafte Ausstellung eines Zertifikats
- Das EPA verweigert dem Zertifikatnehmer den Zugriff auf bestimmte Produkte oder Dienste.

4.4.2. Berechtigung zur Stellung eines Sperrantrags

Einen Antrag auf Sperrung eines Teilnehmerzertifikats können folgende Entitäten stellen:

- der Inhaber des Zertifikats (Zertifikatnehmer)
- der Arbeitgeber des Zertifikatnehmers
- die RA für das EPA
- die CA für das EPA
- sonstige vom EPA autorisierte Parteien.

4.4.3. Verfahren zur Stellung eines Sperrantrags

Das EPA legt in seiner CPS das Verfahren zur Stellung eines Sperrantrags fest oder bringt entsprechende Verweise an.

4.4.4. Frist zur Stellung eines Sperrantrags

Das EPA legt in seiner CPS die Frist für die Stellung eines Sperrantrags fest oder bringt entsprechende Verweise an.

4.4.5. Bedingungen für die Aussetzung

Die Aussetzung wird von der EPA-PKI nicht unterstützt.

4.4.6. Berechtigung zur Stellung eines Antrags auf Aussetzung

Die Aussetzung wird von der EPA-PKI nicht unterstützt.

4.4.7. Verfahren zur Stellung eines Antrags auf Aussetzung

Die Aussetzung wird von der EPA-PKI nicht unterstützt.

4.4.8. Zeitraum der Aussetzung

Die Aussetzung wird von der EPA-PKI nicht unterstützt.

4.4.9. Häufigkeit der Veröffentlichung der Sperrliste (wo zutreffend)

- Die CA für das EPA gibt ihre Sperrliste alle 24 Stunden neu heraus, selbst wenn diese nicht geändert wurde.
- Gemäß ITU-T-Empfehlung X.509 ist in der Sperrliste angegeben, wann die nächste Veröffentlichung erfolgt. Eine neue Sperrliste kann auch vor dem angegebenen Zeitpunkt veröffentlicht werden.

4.4.10. Erfordernisse für die Überprüfung der Sperrliste

Siehe unter Verpflichtungen der Zertifikatempfänger

4.4.11. Sperrung/Statusüberprüfung via Internet

Keine Angaben

4.4.12. Erfordernisse für die Überprüfung der Sperrung via Internet

Keine Angaben

4.4.13. Sonstige Möglichkeiten, die Sperrung bekannt zu machen

Keine Angaben

4.4.14. Erfordernisse hinsichtlich der Überprüfung sonstiger Möglichkeiten, die Sperrung bekannt zu machen

Keine Angaben

4.4.15. Besondere Erfordernisse hinsichtlich der Kompromittierung von Schlüsseln

Keine Angaben

4.5. Verfahren zur Sicherheitsüberprüfung

Die CA für das EPA legt in ihrer CPS fest, wie normale und außergewöhnliche Ereignisse aufgezeichnet werden, wie Protokolle offline (in Papierform) oder online (elektronisch) geführt werden und wie regelmäßige und Ad-hoc-Kontrollen durchgeführt werden, um die Sicherheit der Betriebsumgebung, seiner Nutzer (also von der CA für das EPA beschäftigtes oder beauftragtes Verwaltungs-und Betriebspersonal) sowie der Betriebsabläufe ständig zu überprüfen. Nachfolgend sind die Mindestanforderungen aufgeführt.

4.5.1. Aufgezeichnete Ereignisdaten

Ereignisprotokolle geben das Ereignis an sich an, die beteiligten Nutzer/Mitarbeiter der CA für das EPA, Datum und Uhrzeit und, soweit zutreffend, den Status des Ereignisses (erfolgreich oder nicht erfolgreich). Genaue Angaben zur Art der protokollierten Ereignisse sind in der CPS enthalten.

4.5.2. Häufigkeit der Protokollverarbeitung

Online-Protokolle werden werktäglich verarbeitet, um tatsächliche oder mutmaßliche Sicherheitsverstöße zu erkennen.

4.5.3. Aufbewahrungsfrist für Prüfprotokolle

Protokolle werden mindestens sieben Jahre aufbewahrt.

4.5.4. Schutz von Prüfprotokollen

Online-Protokolle werden z. B. durch Schreibschutz der jeweiligen Datenträger gegen Manipulation geschützt.

4.5.5. Sicherung von Prüfprotokollen

- Kopien aller Online-Prüfprotokolle werden an einem sicheren Ort außerhalb der Betriebsräume aufbewahrt.
- Innerhalb der Aufbewahrungsfrist können Prüfprotokolle eingesehen werden.

4.5.6. Erfassung von Prüfdaten (intern/extern)

Prüfprotokolle werden auf allen Systemen der EPA-PKI erzeugt.

4.5.7. Mitteilung an den Auslöser eines Ereignisses

Keine Angaben

4.5.8. Beurteilung der Angreifbarkeit

Siehe 2.7.

4.6. Archivierung von Betriebsdaten

Die CA für das EPA legt in ihrer CPS fest, wie das Betriebsdatenarchiv zu erzeugen und zu pflegen ist. Nachfolgend sind die Mindestanforderungen aufgeführt.

4.6.1. Aufgezeichnete Ereignisdaten

Gesammelt werden alle wichtigen Nachweise, über welche die CA für das EPA verfügt, z. B.

- Zertifikatanträge und damit in Verbindung stehende Mitteilungen
- Schriftwechsel und Verträge mit Dritten
- Daten der CA für das EPA zur Zertifikaterneuerung einschließlich Schlüsselkennungen und Zertifikaten der CA für das EPA
- Sperranträge und mit dem Antragsteller und/oder Zertifikatnehmer ausgetauschte Informationen
- Prüfprotokolle einschließlich der Berichte über die Jahresprüfung der CA für das EPA

4.6.2. Aufbewahrungsfrist für archivierte Daten

- Die CA für das EPA stellt sicher, dass archivierte Daten mindestens sieben Jahre aufbewahrt werden.
- Sind die ursprünglichen Datenträger nicht geeignet, die Daten über den geforderten Zeitraum zu speichern, so sorgt die CA für das EPA für die regelmäßige Verlagerung der archivierten Daten auf neue Datenträger.
- Die CA für das EPA hält alle Anwendungen zur Verarbeitung archivierter Daten so lange instand, wie dafür Bedarf besteht.

4.6.3. Schutz des Archivs

Die CA für das EPA stellt sicher, dass keine Entität das Archiv manipulieren oder löschen kann.

4.6.4. Sicherung archivierter Daten

Die CA für das EPA stellt sicher, dass archivierte Daten an einem getrennten, sicheren Ort außerhalb der Betriebsräume aufbewahrt werden.

4.6.5. Erfassung von Archivdaten (intern/extern)

Archivdaten werden intern erfasst.

4.6.6. Zugriff auf Archivdaten und deren Überprüfung

Die CA für das EPA stellt sicher, dass nur autorisiertes Personal Zugriff auf Archivdaten hat.

4.7. Schlüsselwechsel

- Spätestens drei Monate vor Ablauf ihres alten privaten Schlüssels erzeugt die CA für das EPA nach dem Prinzip der verteilten/gemeinsamen Schlüssel ein neues Schlüsselpaar zur Signatur und Überprüfung von Zertifikaten sowie ein Zertifikat der CA für das EPA.

- Beim Wechsel eines Schlüsselpaars der CA für das EPA sind die gleichen Sicherheitsmaßnahmen zu treffen wie bei der Erzeugung des ursprünglichen Schlüssels.
- Die CA für das EPA stellt sicher, dass die nachgeordneten Entitäten in der Vertrauenskette innerhalb der CA für das EPA durch den Austausch des Schlüssels so wenig wie möglich beeinträchtigt werden.

4.8. Wiederherstellung im Kompromittierungs-oder Katastrophenfall

Das EPA entwickelt einen umfassenden Plan zur Aufrechterhaltung der Geschäftsprozesse, um im Katastrophenfall den unterbrechungsfreien und uneingeschränkten Betrieb sicherzustellen. Der Plan zur Aufrechterhaltung der Geschäftsprozesse oder Angaben hierzu sind in der CPS des EPA enthalten.

Bei einer tatsächlichen oder mutmaßlichen Kompromittierung des privaten Schlüssels der CA für das EPA benachrichtigt das EPA unverzüglich alle nachgeordneten Entitäten in der Vertrauenskette innerhalb der CA für das EPA. Bei einer Sperrung des Zertifikats der CA für das EPA sind auch alle nachgeordneten Zertifikate zu sperren.

4.9. Einstellung des Zertifizierungsbetriebs

Die CA für das EPA setzt ihre Zertifikatnehmer mindestens sechs Monate im Voraus vom Ablauf des Zertifikats der CA für das EPA in Kenntnis.

Der Betrieb der CA für das EPA gilt als eingestellt, wenn sie auf Dauer keine Zertifizierungsleistungen mehr erbringt. Dies ist jedoch nicht der Fall, wenn der Betrieb zu einer anderen Organisation verlagert wird oder wenn ein altes Schlüsselpaar der CA für das EPA durch ein neues ersetzt wird.

5. PHYSIKALISCHE, VERFAHRENS-UND PERSONALBEZOGENE SICHERHEITSKONTROLLEN

5.1. Physikalische Kontrollen

Welche physikalischen Kontrollen erforderlich sind, um die Anforderungen der CP sowie gegebenenfalls weitere hierin spezifizierte Anforderungen zu erfüllen, und wie die Aufgaben nach Rollen verteilt sind, um die Durchführung von physikalischen Kontrollen zu erleichtern, ist in der CPS der CA für das EPA angegeben.

5.1.1. Betriebsort und Bauweise

Die CA für das EPA wählt für ihren Betriebsort geschützte Räumlichkeiten, deren Innenund/oder Außenwände sowie Decken und Dächer, über die Unbefugte sonst Zugang erhalten könnten, zumindest aus Mauersteinen, Ziegeln, Beton oder Zuschlagstoffen bestehen. Wände schließen oben und unten mit dem Fußboden bzw. der Decke/dem Dach ab (d. h. sie gehen durch Hängedecken oder -böden hindurch, wo durch Lücken Zugangsmöglichkeiten entstehen könnten).

5.1.2. Physikalischer Zugang

Die CA für das EPA beschränkt den physikalischen Zugang zu ihren Betriebsräumen mit Hilfe von Schlössern, Zutrittskontrollen und gegebenenfalls Einbruchmeldesystemen.

5.1.3. Stromversorgung und Klimatisierung

Die CA für das EPA sorgt am Betriebsort für ausreichenden Schutz der Stromversorgung, um die Gefahr von Fehlfunktionen wichtiger EDV-Geräte infolge von Netzausfall, Impulsspitzen oder Spannungsüberhöhung zu vermindern.
Die CA für das EPA sorgt am Betriebsort für ausreichende Klimatisierung, um die Gefahr von Fehlfunktionen wichtiger EDV-Geräte infolge von Überhitzung zu vermindern.

5.1.4. Schutz vor Wasserschäden

Die CA für das EPA sorgt am Betriebsort für ausreichenden Schutz gegen Überschwemmungen im Gebäudeinneren (sowohl durch Wassereinbruch von außen als auch durch auslaufendes Kühlwasser und/oder Heizungsanlagen), die wichtige Betriebsabläufe beeinträchtigen könnten.

5.1.5. Brandschutz

Die CA für das EPA ergreift am Betriebsort geeignete Maßnahmen zum Brandschutz von Computern, Datenträgern, Ausrüstung und Papierarchiven.

5.1.6. Lagerung von Datenträgern

Die CA für das EPA lagert bewegliche Datenträger an einem sicheren Ort.

5.1.7. Abfallentsorgung

Die CA für das EPA stellt sicher, dass Papierunterlagen und Datenträger mit vertraulichen Informationen auf sicherem Weg entsorgt werden.

5.1.8. Externe Datensicherung

Wichtige Systemdaten, Prüfprotokolldaten und andere vertrauliche Daten werden regelmäßig extern gesichert.

5.2. Verfahrenskontrollen

Die CA für das EPA legt in ihrer CPS fest, welche Verfahrenskontrollen erforderlich sind,

um die Anforderungen der CP sowie gegebenenfalls weitere hierin spezifizierte Anforderungen zu erfüllen, und wie die Aufgaben nach Rollen verteilt sind, um die Durchführung von Verfahrenskontrollen zu erleichtern.

5.2.1. Vertrauenspositionen

Die CA für das EPA legt in ihrer CPS die Vertrauenspositionen innerhalb der sicheren Umgebung fest.

5.2.2. Anzahl der Bearbeiter je Aufgabe

Die CA für das EPA legt in ihrer CPS die Anzahl der Bearbeiter je Aufgabe fest.

5.3. Personalkontrollen

Die CA für das EPA legt in ihrer CPS fest, welche Personalkontrollen erforderlich sind, um die Anforderungen der CP sowie gegebenenfalls weitere hierin spezifizierte Anforderungen zu erfüllen, und wie die Aufgaben nach Rollen verteilt sind, um die Durchführung von Personalkontrollen zu erleichtern.

5.3.1. Erfordernisse hinsichtlich Hintergrund, Qualifikationen, Erfahrungen und Sicherheitsüberprüfung

Die CA für das EPA legt in ihrer CPS fest, welche Anforderungen hinsichtlich Hintergrund, Qualifikationen, Erfahrungen und Sicherheitsüberprüfung von ihr beschäftigtes oder beauftragtes Personal zu erfüllen hat.

5.3.2. Verfahren zur Überprüfung des Hintergrunds

Die CA für das EPA fordert vom gesamten Personal den Nachweis von Identität und Qualifikationen anhand entsprechender Dokumente.

5.3.3. Erfordernisse hinsichtlich der Schulung

Die CA für das EPA stellt sicher, dass das Betriebspersonal richtig geschult wird.

5.3.4. Häufigkeit von Nachschulungen und Erfordernisse

Die CA für das EPA stellt sicher, dass das Betriebspersonal nach Bedarf Nachschulungen erhält.

5.3.5. Häufigkeit und Reihenfolge beim regelmäßigen Tätigkeitswechsel

Die CA für das EPA macht in ihrer CPS Angaben zur Häufigkeit und Reihenfolge beim regelmäßigen Tätigkeitswechsel oder bringt entsprechende Verweise an.

5.3.6. Disziplinarmaßnahmen bei unerlaubten Handlungen

Bei unerlaubten Handlungen, die zur Verletzung der Regelungen der CP, der zugehörigen CPS oder anderer Richtlinien und Verfahren führen, ergreift die CA für das EPA Disziplinarmaßnahmen bis hin zur fristlosen Kündigung.

5.3.7. Erfordernisse im Hinblick auf Vertragspersonal

Die CA für das EPA stellt sicher, dass externe Auftragnehmer oder Berater, die am Betrieb der EPA-PKI beteiligt sind, alle Dienstleistungen mit der gebotenen Sorgfalt erbringen und zu diesem Zweck ausreichend qualifiziertes Personal einsetzen.

5.3.8. Unterlagen für das Personal

Die CA für das EPA stellt sicher, dass das gesamte am CA-Betrieb mitwirkende Personal die erforderlichen Handbücher, Arbeitsanweisungen und/oder technischen Spezifikationen erhält.

6. TECHNISCHE SICHERHEITSKONTROLLEN

6.1. Erzeugung und Installation von Schlüsselpaaren

6.1.1. Erzeugung von Schlüsselpaaren

- Die CA für das EPA verwendet ein oder mehrere eigenständige hardwarebasierte kryptografische Module, welche in Bezug auf die Erzeugung von Schlüsselpaaren zur Signierung und Verifizierung von Zertifikaten den Standard FIPS PUB 140-1 zumindest bis zur Sicherheitsstufe 3 erfüllen und entsprechend zertifiziert sind.
- Teilnehmerschlüsselpaare werden von der CA für das EPA auf Smartcards erzeugt.

6.1.2. Auslieferung privater Schlüssel an Entitäten

Private Schlüssel werden von der CA für das EPA erzeugt, auf Smartcards gespeichert und an den jeweiligen Zertifikatnehmer ausgeliefert.

6.1.3. Auslieferung öffentlicher Schlüssel an den Zertifikatausssteller

Öffentliche Schlüssel erhält die CA für das EPA nach einer Zertifikatanforderung gemäß PKCS#10.

6.1.4. Auslieferung des öffentlichen Schlüssels der CA für das EPA sowie der CRL an berechtigte Nutzer

Den öffentlichen Schlüssel der CA für das EPA bekommen berechtigte Nutzer auf Anfrage über ein dauerhaftes Kommunikationsmittel wie das Internet. Wo die CRL bereitgestellt wird, ist in der CPS festgelegt.

6.1.5. Schlüssellänge

Die Schlüssel der CA für das EPA weisen eine Länge von mindestens 2 048 Bit auf. Teilnehmerschlüssel weisen eine Länge von mindestens 1 024 Bit auf.

6.1.6. Erzeugung der Parameter für öffentliche Schlüssel

Keine Angaben

6.1.7. Überprüfung der Parameterqualität

Keine Angaben

6.1.8. Erzeugung von Hardware-/Softwareschlüsseln

Die Schlüssel der CA für das EPA werden in einem kryptografischen Modul erzeugt, welches den Standard FIPS PUB 140-1 zumindest bis zur Sicherheitsstufe 3 erfüllt.

6.1.9. Schlüsselnutzungszweck (gemäß X.509 v3, Feld "KeyUsage")

Bei Zertifikaten gemäß ITU-T Standard X.509, Version 3 wird die Zertifikaterweiterung KeyUsage im Einklang mit RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile verwendet.

6.2. Schutz privater Schlüssel

6.2.1. Standards für das kryptografische Modul

Die CA für das EPA verwendet ein hardwarebasiertes kryptografisches Modul, welches in Bezug auf den Schutz ihrer privaten Schlüssel den Standard FIPS PUB 140-1 zumindest

bis zur Sicherheitsstufe 3 erfüllt und entsprechend zertifiziert ist.

6.2.2. Kontrolle privater Schlüssel durch mehrere (n von m) Personen

Der Zugang zu den privaten Schlüssel der CA für das EPA ist auf mehrere Personen verteilt. Mindestens n von m Personen sind erforderlich, um Zugang zu den Schlüsseln zu erhalten. In ihrer CPS macht die CA für das EPA Angaben zu den im Einzelnen implementierten Kontrollmechanismen.

6.2.3. Hinterlegung privater Schlüssel bei Dritten

In der EPA-PKI werden Schlüssel nicht bei Dritten hinterlegt.

6.2.4. Sicherung privater Schlüssel

Die CA für das EPA stellt sicher, dass das System verteilter/gemeinsamer Schlüssel die Wiederherstellung privater Schlüssel unterstützt, damit nach einem Katastrophenfall der Wiederanlauf des Betriebs gewährleistet werden kann.

6.2.5. Archivierung privater Schlüssel

Abgelaufene, nicht mehr aktive private Signaturschlüssel werden nicht archiviert, sondern gemäß Abschnitt 6.2.9 vernichtet.

6.2.6. Transfer privater Schlüssel in das kryptografische Modul

Die CA für das EPA stellt sicher, dass im Rahmen des Systems verteilter/gemeinsamer Schlüssel private Schlüssel auf sicherem Weg in das kryptografische Modul transferiert werden.

6.2.7. Verfahren zur Aktivierung privater Schlüssel

Die CA für das EPA stellt sicher, dass im Rahmen des Systems verteilter/gemeinsamer Schlüssel private Schlüssel wirksam und sicher aktiviert werden.

6.2.8. Verfahren zur Deaktivierung privater Schlüssel

Die CA für das EPA stellt sicher, dass private Schlüssel von CA, RA und Zertifikatnehmern ordnungsgemäß deaktiviert werden.

6.2.9. Verfahren zur Vernichtung privater Schlüssel

Die CA für das EPA stellt sicher, dass ihre deaktivierten privaten Schlüssel unwiderruflich vernichtet werden.

6.3. Sonstige Aspekte der Verwaltung von Schlüsselpaaren

6.3.1. Archivierung öffentlicher Schlüssel

Zu Archivierungszwecken bewahrt die CA für das EPA Kopien aller öffentlichen Teilnehmerschlüssel auf.

6.3.2. Gültigkeitsdauer öffentlicher und privater Schlüssel

Schlüssel der CA für die Europäische Patentorganisation gelten 20 Jahre.
Schlüssel der CA für das EPA gelten 10 Jahre.
Teilnehmerschlüssel gelten 3 Jahre.

6.4. Aktivierungsdaten

6.4.1. Erzeugung und Installation von Aktivierungsdaten

Um nach Bedarf den Zugang zu Computern, Geräten und physikalischen Bereichen am

Betriebsort zu kontrollieren, verwendet die CA für das EPA Aktivierungsdaten wie Passwörter oder PINs.

6.4.2. Schutz von Aktivierungsdaten

Die CA für das EPA stellt sicher, dass im Hinblick auf den Schutz von Passwörtern und PINs geeignete Richtlinien für ihr Personal (Führungskräfte und Sachbearbeiter, die im Dienst der CA für das EPA stehen oder in ihrem Auftrag tätig sind) festgelegt und angewendet werden.

6.4.3. Sonstige Aspekte im Zusammenhang mit Aktivierungsdaten

Keine Angaben

6.5. Sicherheitsmaßnahmen für Computer

6.5.1. Besondere technische Anforderungen an die Computersicherheit

Die CA für das EPA führt gegebenenfalls Kontrollen zur Computersicherheit durch, um den einzelnen Nutzer zu identifizieren, mit Hilfe von Passwort oder PIN seine Authentizität festzustellen, den Zugang des Nutzers zu Daten und Funktionen entsprechend seinen Aufgaben und Berechtigungen zu begrenzen und sicherheitsrelevante Ereignisse in einem Online-Protokoll (Prüfungsschiene) festzuhalten.

6.5.2. Einstufung der Computersicherheit

Nicht zutreffend. Siehe Abschnitt 6.1.1.

6.6. Technische Kontrollen während der Lebensdauer

6.6.1. Kontrollen bei der Systementwicklung

Während der Entwicklung führt die CA für das EPA gegebenenfalls Kontrollen durch, um sicherzustellen, dass die Erzeugung, Integration, Erprobung, Konfiguration, Installation, Inbetriebnahme und Wartung von Software und Hardware im Einklang mit den Geschäftszielen der CA für das EPA erfolgt. Für Kaufteile werden geeignete Wareneingangsverfahren angewandt.

6.6.2. Kontrollen im Rahmen des Sicherheitsmanagements

Die CA für das EPA baut ein Sicherheitssystem auf und leitet und kontrolliert alle Sicherheitsmaßnahmen bezüglich Systementwicklung und –betrieb.

6.6.3. Sicherheitseinstufung während der Lebensdauer

Nicht zutreffend.

6.7. Kontrolle der Netzsicherheit

Die CA für das EPA schützt ihr internes Kommunikationsnetz gegen unbefugten Zugriff, einschließlich des Zugriffs über angeschlossene externe Netze. Jede derartige Verbindung wird durch eine eigene Firewall geschützt. Unter Beachtung der jeweiligen Sicherheitsvorgaben wird jede Firewall so konfiguriert, dass der Datenverkehr zwischen den Netzen auf ein zur Erreichung der Geschäftsziele unbedingt erforderliches Maß begrenzt wird und eingehende Daten gegebenenfalls auf Virenbefall überprüft werden. Die Firewalls werden regelmäßigen und Ad-hoc-Kontrollen unterzogen, um tatsächliche oder mutmaßliche Sicherheitsverstöße zu erkennen.

6.8. Kontrolle der technischen Ausführung des kryptografischen Moduls

Keine Angaben

7. PROFIL VON ZERTIFIKATEN UND SPERRLISTEN

Gemäß PCT, Anhang F handelt es sich bei Teilnehmerzertifikaten um "Low-Level-Zertifikate".

7.1. Profil von Zertifikaten

Teilnehmerzertifikate entsprechen den Anforderungen gemäß RFC 2459.

7.1.1. Versionsnummer(n)

Zertifikate der CA für das EPA und Teilnehmerzertifikate entsprechen dem Standard X.509, Version 3.

7.1.2. Zertifikaterweiterungen

Die CA für das EPA implementiert eine einzige nicht kritische, CP-bezogene Zertifikaterweiterung gemäß RFC 2459, wobei jedes Zertifikat so genannte CP-Qualifier enthält.

7.1.3. Object Identifier für Algorithmen

Es werden Object Identifier gemäß RFC 2459 verwendet.

7.1.4. Namensformen

Siehe 3.1.1.

7.1.5. Namensbeschränkungen

Keine Angaben

7.1.6. Object Identifier der Zertifizierungsrichtlinie

Siehe Abschnitt 1.2.

7.1.7. Erweiterung zur beschränkten Anwendbarkeit der Richtlinie

Keine Angaben

7.1.8. Syntax und Semantik von Richtlinienkennungen

Keine Angaben

7.1.9. Semantische Abarbeitung von kritischen CP-Erweiterungen

Keine Angaben

7.2. Sperrlistenprofil

7.2.1. Versionsnummer(n)

Im Einklang mit dieser Richtlinie veröffentlichte Sperrlisten werden gemäß ITU-T X.509 und RFC 2459 erstellt.

7.2.2. Erweiterungen für Sperrlisten und Sperrlisten-Einträge

Keine Angaben

8. VERWALTUNG DER RICHTLINIE

8.1. Änderung der Richtlinie

Bei Änderung der Richtlinie wird ein Dokument mit der geänderten oder aktualisierten Fassung veröffentlicht.

8.2. Veröffentlichung und Mitteilungen

Zu Einzelheiten siehe Abschnitt 1.4.

8.3. Genehmigungsverfahren

Dieses Dokument wird vom Direktorat Sicherheit und Audit des EPA gepflegt.