# Erklärung zum Zertifizierungsbetrieb des Europäischen Patentamts

**Version 1.10**

**Gültig ab: 1. Januar 2011**

European Patent Office
Bayerstrasse 35
80335 München
Deutschland
Tel.: +31 70 340 4500
http://www.epo.org

**Erklärung zum Zertifizierungsbetrieb des Europäischen Patentamts**

© Europäisches Patentamt, 2004 -2011. Alle Rechte vorbehalten.

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 Erklärung zum Zertifizierungsbetrieb des EPA wenden Sie sich bitte an: eBusiness User Support, European Patent Office, Bayerstrasse 35, 80335 München,

Deutschland,E-Mail: support@epo.org

**Copyright**
Die korrekte Wiedergabe von Inhalten dieses Dokuments ist mit Quellenangabe gestattet, es sei denn, es wird auf eine Nutzungseinschränkung bzw. ein besonderes Genehmigungserfordernis hingewiesen.

**Logo**
Das EPA-Logo ist als amtliches Zeichen einer internationalen Organisation nach der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums weltweit geschützt.

**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 | 1. März 2008 | Freigabe des Dokuments |
| 1.10 | 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

| | Deutsch |
|---|---|
| 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 |
| CDS | Kundendatenbanksystem (Client Database System) |
| CMS | Card-Managementsystem |
| 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 Name (Distinguished Name) |
| EPA | Europäisches Patentamt |
| EPA-PKI | Public-Key-Infrastruktur des Europäischen Patentamts |
| EPÜ | Europäisches Patentübereinkommen |
| FREP | Vertreter, die Einreichung durchführt (Filing Representative) |
| 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 |

# LITERATURLISTE

In dieser Erklärung zum Zertifizierungsbetrieb 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

[RFC2527] 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.

[CP] Certificate Policy, Zertifizierungsrichtlinie des Europäischen Patentamts

[RPA] Relying Party Agreement, Verpflichtungserklärung des Zertifikatempfängers

[SA] Subscriber Agreement, Verpflichtungserklärung des Zertifikatnehmers

# 1. EINFÜHRUNG IN DIE ERKLÄRUNG ZUM ZERTIFIZIERUNGSBETRIEB DES EUROPÄISCHEN PATENTAMTS

## 1.1. Übersicht

Diese Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) ergänzt die Zertifizierungsrichtlinie (Certificate Policy, CP) des Europäischen Patentamts. Beide Dokumente stützen die Public-Key-Infrastruktur des Europäischen Patentamts (EPA-PKI) und entsprechen dem in RFC 2527 vorgeschlagenen Format.

Während die CP die Erfordernisse der EPA-PKI beschreibt, geht die CPS noch darüber hinaus; sie beschreibt die Verfahren, die das EPA zur Ausstellung, Nutzung und Sperrung von Teilnehmerzertifikaten im Rahmen der EPA-PKI anwendet, um die Anforderungen gemäß CP zu erfüllen.

Inhaltlich werden einige Teile der CP in der CPS wieder aufgegriffen. Dies ist dann der Fall, wenn die CPS keine weitere Ausführung oder Klärung des CP-Inhalts erfordert. Zur Kenntlichmachung sind die Textwiederholungen in der CPS kursiv gedruckt.

### 1.1.1. Das Europäische Patentamt und seine Online-Dienste

Das Europäische Patentamt (EPA) ist das ausführende Organ der EuropäischenPatentorganisation. Es wurde durch das Europäische Patentübereinkommen (EPÜ) gegründet und ist mit verwaltungsmäßiger und finanzieller Selbstständigkeit 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.
Diese Erklärung zum Zertifizierungsbetrieb des Europäischen Patentamts (CPS) beschreibt die Verfahren, die das EPA zur Ausstellung, Nutzung und Sperrung von Teilnehmerzertifikaten im Rahmen der EPA-PKI anwendet.

### 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 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 für gesperrte Zertifikate
- 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 (Einzelheiten hierzu siehe CP) verlassen können.

Wie in der CP festgelegt, behält das EPA zwar die Verantwortung für alles, was die EPAPKI betrifft, einige Teile des EPA-PKI-Betriebs allerdings haben externe Dienstleister übernommen, so z. B. die Leitung und Verwaltung der Dienste der CA für das EPA und die Organisation der Smartcard-Ausgabe an Dritte.

### 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 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 Präsidentindes 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 "Erklärung zum Zertifizierungsbetrieb 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. Umdiese 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 (CA für das EPA). Diese stellt alle Teilnehmerzertifikate aus. Das Zertifikat der CA für das EPA selbst wurde von der CA 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 Registrierungsstelle (RA) für das EPA ist für die Identifizierung und Authentifizierung von Antragstellern innerhalb der EPA-PKI zuständig.

Die CA für das EPA unterscheidet zwischen zwei Gruppen von Zertifikatnehmern:

- Zertifikatnehmer, die dem EPA bei Beantragung einer Smartcard als registrierte Teilnehmer mit einer FREP-Nummer bekannt sind, z. B. zugelassene Vertreter, deren Mitarbeiter, Rechtsanwälte. Diese Zertifikatnehmer haben Zugriff auf alle Online-Dienste des EPA.

- Zertifikatnehmer, die dem EPA zum Zeitpunkt der Beantragung einer Smartcard unbekannt sind, z. B. erstmalig aktiv werdende Anmelder oder Vertreter. Diese Zertifikatnehmer haben nur Zugriff auf das Anwendungsprogramm für die Online-Einreichung.

#### 1.3.3. Zertifikatempfänger

##### 1.3.3.1. EPA

Im Sinne der CP gilt das EPA als Zertifikatempfänger.

#### 1.3.3.2. Anmeldeamt

Andere Entitäten können Zertifikatempfänger sein, sofern sie unter dem PCT (siehe Art. 10 PCT) als Anmeldeamt in Frage kommen, in dieser Eigenschaft 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.

#### 1.3.3.3. Zentralbehörde für den gewerblichen Rechtsschutz

Andere Entitäten können Zertifikatempfänger sein, sofern sie als Zentralbehörde für dengewerblichen Rechtsschutz 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 von der betreffenden Zentralbehörde für den gewerblichen Rechtsschutz zu erfüllen sind.

#### 1.3.3.4. 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.

### 1.3.4. 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 Erklärung zum Zertifizierungsbetrieb

Die Erklärung zum Zertifizierungsbetrieb 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, Germany, *E-Mail: support@epo.org*

### 1.4.3. Überprüfung der Konformität von CPS und CP

Ob die CPS mit der CP in Einklang steht, ermittelt das in Abschnitt 1.4.1, Verwaltung der Erklärung zum Zertifizierungsbetrieb, genannte Gremium.

## 1.5. Inkrafttreten/Übergangsrecht

Die CPS ist an dem Tag in Kraft getreten, der auf dem Deckblatt als Gültigkeitsdatum angegeben ist.

Das in der CPS 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 bestätigt, dass für die EPA-PKI die Bedingungen der CPS rückwirkend ab diesem Gültigkeitsdatum gelten.

Sofern in der CPS 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 CPS ab dem Datum, das auf dem revidierten Dokument angegeben ist.

# 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 im Hinblick auf die Zugangs-und Nutzungskontrolle stellt sie eine geschützte Umgebung 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: Auf diesen Verzeichnisdienst haben nur berechtigte Nutzer Zugriff.)
- Sie erzeugt Schlüsselpaare für Zertifikatnehmer auf der jeweiligen Smartcard, leitet die Zertifikatanträge zur Zertifizierung weiter, speichert das Zertifikat auf der Smartcard ab und verschickt Smartcard und Smartcard-PIN an den Zertifikatnehmer.
- Sie erzeugt eine Liste der gesperrten Zertifikate und veröffentlicht diese im entsprechenden 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 dieser 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 sie.
- 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. 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, ob für einen bestimmten Zweck die Verwendung eines Zertifikats zweckdienlich ist und ob ein Zertifikat tatsächlich für den vorbestimmten Zweck eingesetzt wird.
- Vor der Verifizierung eines vorgelegten Zertifikats überprüft er dieses auf Sperrung oder Aussetzung.

### 2.1.5. Verpflichtungen des Verzeichnisdienstes

Der Verzeichnisdienst der CA für das EPA unterliegt der Verantwortung des EPA. Bei Sperrung eines Teilnehmerzertifikats veröffentlicht die CA für das EPA im Sperrverzeichnis eine entsprechende Mitteilung.

## 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 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 die Sperrung von Zertifikaten sowie die Herausgabe von Sperrlisten 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 den gewerblichen Rechtsschutz 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-oder 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 der CP), 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 auszulegen, dass die Rechte der Europäischen Patentorganisation aus dem am 5. Oktober 1973 in München unterzeichneten Europäischen Patentübereinkommen (EPÜ) einschließlich des Protokolls über die Vorrechte und Immunitäten der EPO in jedem Fall 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 zu 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. Der Ort des schiedsrichterlichen Verfahrens ist München.

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 Rechtsmittel 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 (zumindest auf einer Website im Internet):

- Zertifizierungsrichtlinie des EPA
- Erklärung zum Zertifizierungsbetrieb des EPA
- Zertifikat der CA für die Europäische Patentorganisation (Wurzelzertifikat)
- Verpflichtungserklärung des Zertifikatempfängers
- Verpflichtungserklärung des Zertifikatnehmers
- 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. Verzeichnisdienst

Im Hinblick auf die Veröffentlichung von Teilnehmerzertifikaten, Sperrlisten sowie Dokumenten zur EPA-PKI 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 daher nur dem EPA bekannt gemacht.

## 2.8. Vertraulichkeit

### 2.8.1. Vertrauliche 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 Inhabers

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

Die CA für das EPA verwendet in den Feldern "Issuer" und "Subject" Distinguished Names (DN) gemäß X.501 (siehe Tabelle 1):

| Attribut | Wert |
|---|---|
| Country (C)= | NL |
| Organisation (O)= | European Patent Office |
| Organisational Unit (OU)= | Nicht verwendet |
| State or Province (S)= | Nicht verwendet |
| Locality (L)= | Nicht verwendet |
| Common Name (CN) | European Patent Office CA |

**Tabelle 1 - Attribute für Distinguished Name im Zertifikat der CA für das EPA**

Teilnehmerzertifikate, die von der CA für das EPA ausgestellt werden, enthalten in Einklang mit Abschnitt 7.1 einen Distinguished Name gemäß X.501.

### 3.1.2. Aussagekraft von Namen

Die RA für das EPA stellt sicher, dass ein Attributsatz einen Zertifikatnehmer eindeutig identifiziert und aussagekräftige Werte enthält; hierzu fügt sie eine eindeutige vierstellige Kennung an.

### 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 Distinguished Name 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 vermeidet die CA für das EPA dadurch, dass sie jedem Antragsteller eine eindeutige Nummer zuweist, um die Eindeutigkeit von Common Name (CN) und Distinguished Name (DN) sicherzustellen.

### 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 RA für das EPA prüft, ob die Organisation des Anmelders im Kundendatenbanksystem

(Client Data System, CDS) des EPA geführt wird.

### 3.1.9. Authentifizierung der Identität von Einzelpersonen

In Fällen, wo das EPA einem neuen Zertifikatnehmer bereits eine FREP-Nummer zugeteilt hat, wird die Identität des Antragstellers von der RA für das EPA authentifiziert, die dessen Angaben zur Person im CDS überprüft.

Sind im CDS keine Referenzen für den Anmelder gespeichert, muss die RA für das EPA seine Identität durch Überprüfung folgender Angaben zur Person authentifizieren:

- Vorname(n)
- Nachname
- Anschrift
- E-Mail-Adresse
- Pass-oder Ausweisnummer
- Unterschrift des Zertifikatnehmers auf dem per Fax übermittelten Registrierungsformular

Die RA für das EPA erklärt den Zertifikatantrag für gültig, indem sie die Datei mit den Angaben des neuen Zertifikatnehmers in das Smartcard-Managementsystem lädt.

## 3.2. Schlüsselerneuerung im Normalfall

Wurden die Zertifikate eines Zertifikatnehmers nicht gesperrt, so erhält er sechzig Tage vor Ablauf von der CA für das EPA per E-Mail die Aufforderung, seine Zertifikate zu erneuern. Der Zertifikatnehmer wird auf die Registrierungswebsite weitergeleitet, und nach Überprüfung seiner Identität kann er neue Zertifikate beantragen. Die Identität des Zertifikatnehmers wird anhand seines derzeit gültigen Zertifikats überprüft.

Die CA für das EPA erzeugt neue Schlüssel auf einer neuen Smartcard und schickt diese zusammen mit einem Bestätigungsschreiben an den Zertifikatnehmer. Der Zertifikatnehmer sendet das Bestätigungsschreiben an die RA für das EPA zurück, und nach dessen Erhalt aktivieren CA und RA für das EPA die Zertifikate.

## 3.3. Schlüsselerneuerung nach Sperrung

Zur Schlüsselerneuerung nach einer Sperrung ist im Hinblick auf Identifizierung und Authentifizierung wie bei der Erstregistrierung zu verfahren.

Die Schlüsselerneuerung nach einer Sperrung ist nicht zulässig, wenn

- das gesperrte Zertifikat auf eine andere Person ausgestellt wurde,
- für die RA des EPA Grund zur Annahme besteht, dass falsche Angaben zur Person gemacht wurden.

## 3.4. Antrag auf Sperrung

Bevor ein Zertifikat gesperrt wird, authentifiziert die RA für das EPA die Identität des Antragstellers durch Überprüfung

- der Angaben zur Person des Antragstellers (dies kann der Zertifikatnehmer oder dessen Arbeitgeber sein).

# 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 geboten Sorgfalt vor. Die CA für das EPA dokumentiert die 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 deutlich 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

### 4.2.1. Erzeugung von Schlüsseln

Schlüssel werden gemäß Abschnitt 6.1 dieser CPS auf einer Smartcard erzeugt.

### 4.2.2. Speicherung im Token

Schlüssel werden auf der nutzerspezifischen Smartcard des Zertifikatnehmers gespeichert.

### 4.2.3. Erzeugung von Zertifikaten

Sobald die Datei mit den Daten des neuen Zertifikatnehmers im Smartcard-Managementsystem (CMS) geladen ist, wird ein Zertifikatantrag gemäß PKCS#10 erzeugt und an die CA für das EPA übermittelt. Nach Eingang einer PKCS#7-Rückmeldung der CA für das EPA speichert das Smartcard-Managementsystem das Zertifikat auf der Smartcard ab.

### 4.2.4. Erzeugung von PINs

Sobald das Zertifikat auf der Smartcard gespeichert ist, wird für die Nutzer-PIN ein Zufallswert ausgewählt.

### 4.2.5. Verteilung und Auslieferung

Die CA für das EPA schickt dem neuen Zertifikatnehmer innerhalb von 10 Tagen nach Antragsgenehmigung ein Paket mit einer nutzerspezifischen Smartcard, einem Smartcard-Lesegerät, einem Startpaket für die Online-Dienste auf CD, dem Bestätigungsschreiben sowie weiterer Dokumentation des EPA.

## 4.3. Abnahme und Aktivierung von Zertifikaten

Der Zertifikatnehmer muss den Erhalt seiner Smartcard bestätigen; dazu unterzeichnet er das Bestätigungsschreiben und faxt es an die CA für das EPA. Mit dieser Bestätigung gilt das Zertifikat als abgenommen.

Nach Eingang des unterzeichneten Bestätigungsschreibens bei der CA für das EPA erhält der Zertifikatnehmer seine PIN, und über eine sichere Verbindung wird eine LDIF-Datei an die RA für das EPA geschickt. Die RA für das EPA aktiviert das Zertifikat, indem sie es in Form dieser LDIF-Datei in das Verzeichnis lädt. Sobald das Teilnehmerzertifikat im Verzeichnis geladen ist, kann der Zertifikatnehmer die Online-Dienste des EPA nutzen.

Wird das Bestätigungsschreiben nicht innerhalb von 8 Wochen zurückgeschickt, so verwirft der CMS-Administrator den Antrag auf Ausstellung einer Smartcard.

## 4.4. Sperren von Zertifikaten

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

### 4.4.1. Bedingungen für die Sperrung

#### 4.4.1.1. Teilnehmerzertifikate

Die Sperrung eines Zertifikats kann vom Zertifikatnehmer (oder anderen Personen gemäß Abschnitt 4.4.2) 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
- (z. B. Namensänderung bei Heirat) 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.
- Ausscheiden des Zertifikatnehmers aus dem Unternehmen oder der Organisation.

#### 4.4.1.2. CA-Zertifikate

Das EPA sperrt ein CA-Zertifikat, das in seinen Zuständigkeitsbereich fällt, wenn es feststellt oder Grund zur der Annahme hat, dass der private Schlüssel dieser CA kompromittiert wurde,

ein autorisierter EPA-Bediensteter die Sperrung des Zertifikats beantragt.

### 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

Anträge auf Sperrung von CA-Zertifikaten werden nur von Parteien angenommen, die hierzu vom EPA autorisiert sind.

### 4.4.3. Verfahren zur Stellung eines Sperrantrags

Sperranträge reicht der Zertifikatnehmer (oder sein Arbeitgeber) per E-Mail, Fax oder Post bei der RA für das EPA ein. Die RA für das EPA prüft, ob der Sperrantrag von einer im Hinblick auf das jeweilige Zertifikat autorisierten Partei eingereicht wurde, und schickt dann ihrerseits einen Sperrantrag an die CA für das EPA.

Die CA für das EPA bearbeitet den Antrag während ihrer Dienstzeiten und veröffentlicht das gesperrte Zertifikat in der Sperrliste. Die RA für das EPA unterrichtet dann den Zertifikatnehmer per E-Mail von der Sperrung.

### 4.4.4. Frist zur Bearbeitung eines Sperrantrags

Die RA für das EPA ergreift alle geeigneten Maßnahmen, um die Bearbeitung von Sperranträgen innerhalb eines akzeptablen Zeitrahmens sicherzustellen.

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

- Die CA für die Europäische Patentorganisation gibt ihre Sperrliste alle drei Monate neu heraus oder aber, wenn das Zertifikat einer ihrer nachgeordneten Zertifizierungsstellen gesperrt wurde.

### 4.4.10. Verpflichtung zur Überprüfung der Sperrliste

Entsprechend der Verpflichtungserklärung des Zertifikatempfängers [RPA] hat dieser vor der Verifizierung eines vorgelegten Zertifikats für die gesamte Zertifikatkette zu überprüfen, ob ein Zertifikat gesperrt oder ausgesetzt wurde.

### 4.4.11. Sperrung/Statusüberprüfung via Internet

Keine Angaben

### 4.4.12. Erfordernisse hinsichtlich 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

Folgende Ereignisse werden von der CA für das EPA manuell oder automatisch protokolliert:

### 4.5.1. Aufgezeichnete Ereignisse

- Ereignisse in den einzelnen Phasen der CA-Schlüsselverwaltung, einschließlich:
  - Erzeugung, Sicherung, Speicherung, Wiederherstellung, Archivierung und Vernichtung von Schlüsseln
  - Ereignisse in den einzelnen Phasen der Verwaltung kryptografischer Geräte
- Ereignisse in den einzelnen Phasen der Verwaltung von CA-und Teilnehmerzertifikaten, einschließlich:
  - Beantragung, Verlängerung, Erneuerung und Sperrung von Zertifikaten
  - Bearbeitung von Anträgen mit positivem oder negativem Ausgang
  - Erzeugung und Ausstellung von Zertifikaten und Sperrlisten
- Sicherheitsrelevante Ereignisse, einschließlich:
  - erfolgreiche und erfolglose Zugriffsversuche auf das PKI-System
  - Maßnahmen an PKI und Sicherheitssystem, die von Personal der Firma Getronics PinkRoccade (GPR) durchgeführt wurden
  - Lesen, Speichern oder Löschen von vertraulichen Dateien oder Datensätzen
  - Änderungen am Sicherheitsprofil
  - Systemabstürze, Hardware-Ausfälle und sonstige Unregelmäßigkeiten
  - Firewall-und Router-Aktivität
  - Besucherverkehr in den Räumen der CA

Protokolleinträge beinhalten folgende Angaben:

- Datum und Uhrzeit des Eintrags

- bei automatisch erzeugten Protokolleinträgen die fortlaufende Nummer des Eintrags
- Identität der eintragenden Entität
- Art des Eintrags.

RA für das EPA und Administratoren protokollieren Registrierungsdaten zum Zertifikat, einschließlich:

- Art der vom Zertifikatnehmer vorgelegten Ausweispapiere
- Datensatz mit eindeutigen Identifizierungsdaten, Nummern von Ausweispapieren (z. B. Führerscheinnummer), gegebenenfalls auch in Kombination
- Ort, an dem Kopien von Anträgen und Ausweispapieren abgelegt sind
- Identität der Entität, die den Antrag angenommen hat
- ggf. zur Validierung von Ausweispapieren angewandtes Verfahren
- ggf. Name der CA, die den Antrag entgegengenommen hat, oder der RA, die ihn gestellt hat

Darüber hinaus stellt das CMS umfangreiche Dateien mit Betriebs-und Prüfprotokollen bereit, aus denen alle durchgeführten Operationen sowie die Identität des Nutzers, der die jeweilige Operation angestoßen hat, hervorgehen. Es können Berichte mit folgenden Angaben erstellt werden:

- General Data – alle Arbeitsschritte sind über Suchkriterien einsehbar
- List Devices – in einer druckbaren Liste wird angezeigt, wer gerade welches Gerät hat
- Certificate Request – Überprüfung von Zertifikatanträgen, die der CA für das EPA übermittelt wurden
- Issued Certificates – Überprüfung und Sperrung bereits ausgestellter Zertifikate
- Revoked Certificates – Überprüfung von Sperranträgen
- Add/Modify/Remove Users – Hinzufügen/Ändern/Entfernen von Nutzern
- Issue/Change/Cancel Cards – Ausstellen/Ändern/Sperren von Smartcards
- Modify System Configuration – Ändern der Systemkonfiguration

### 4.5.2. Häufigkeit der Protokollbearbeitung

Online-Protokolle werden werktäglich verarbeitet, um tatsächliche oder mutmaßliche Verstöße gegen die Sicherheitsbestimmungen zu erkennen.

### 4.5.3. Aufbewahrungsfrist für Prüfprotokolle

Protokolle sind mindestens sieben Jahre aufzubewahren.

### 4.5.4. Schutz von Prüfprotokollen

Online-Protokolle sind z. B. durch Schreibschutz der jeweiligen Datenträger gegen Manipulation zu schützen, und Prüfprotokolle sind so zu schützen, dass nur autorisiertes Personal darauf zugreifen kann.

Bei einer externen Prüfung werden keine Daten nach außen transferiert, und eine Überprüfung der Daten ist nur unter Aufsicht von EPA-Personal oder EPA-Vertragspersonal gestattet.

Elektronisch archivierte Daten sind durch physikalische und logische Zugangskontrollen gegen unerlaubte Einsichtnahme, Änderung, Löschung oder sonstige Eingriffe 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

Das EPA führt regelmäßig eine Beurteilung der Angreifbarkeit seiner CA-und RA-Systeme durch. Auf Grundlage der Beurteilungsergebnisse werden Richtlinien, Verfahrensweisen und Systemkonfigurationen entsprechend angepasst.

## 4.6. Archivierung von Betriebsdaten

### 4.6.1. Archivierte 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
- alle in Abschnitt 4.5.1 aufgeführten Ereignisarten

### 4.6.2. Aufbewahrungsfrist für archivierte Daten

- Alle Prüfprotokolle werden nach ihrer Erstellung sieben Jahre lang aufbewahrt.
- Sind die ursprünglichen Datenträger nicht geeignet, die Daten über den geforderten Zeitraum zu speichern, so stellt die CA für das EPA die regelmäßige Verlagerung der archivierten Daten auf neue Datenträger sicher.
- Die CA für das EPA hält alle Anwendungen zur Verarbeitung archivierter Daten so lange instand, wie diese Daten möglicherweise gebraucht werden.

### 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. Sicherungskopien von archivierten 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 Schlüsselwechsel so wenig wie möglich beeinträchtigt werden.

## 4.8. Wiederherstellung im Kompromittierungs-oder Katastrophenfall

Um im Katastrophenfall den unterbrechungsfreien und uneingeschränkten Betrieb sicherzustellen, hat das EPA anwendungs-und systemspezifische Pläne zur Aufrechterhaltung der Geschäftsprozesse und Wiederherstellung im Katastrophenfall umgesetzt. Siehe Service Continuity Plan (Plan zur Aufrechterhaltung des Betriebs) der Hauptdirektion Informationsmanagement.

### 4.8.1. Schlüsselkompromittierung

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.

### 4.8.2. Wiederherstellung im Katastrophenfall

Die CA für das EPA hat eine externe Einrichtung zur Wiederherstellung im Katastrophenfall geschaffen. Um die Wiederherstellung gewährleisten zu können, wurde Folgendes umgesetzt:

- Umfassend dokumentiertes System, einschließlich Entwurf, Konfigurationsdateien und detaillierte Installationsskripts für Systeme, Hardware und Software
- Sicherungs-und Wiederherstellungsprozeduren; Sicherungskopien werden an zwei verschiedenen Orten gespeichert
- Klone der kryptografischen Hardware – zwei auf verschiedenen Signaturservern implementierte Klone dienen als gegenseitige Live Backups

## 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 trifft jedoch nicht zu, 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

Die CA für das EPA, einschließlich der Abteilung für die Smartcard-Verarbeitung (mit dem Smartcard-Managementsystem, CMS) ist an einem sicheren Ort außerhalb der Diensträume des EPA in den Niederlanden untergebracht.

Die RA für das EPA befindet sich in den Diensträumen des EPA in München. Diese CPS unterstützt die Sicherheitsanforderungen, wie sie in der Zertifizierungsrichtlinie des Europäischen Patentamts festgelegt sind. Alle Aktivitäten von CA und RA sind in einer physikalisch geschützten Umgebung durchzuführen, die versteckt oder offen agierende Eindringlinge abschrecken, fernhalten und erkennen soll.

### 5.1.1. Betriebsort und Bauweise

Informationsträger mit Angaben zu Betriebsort und Bauweise sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde. Betriebsort der CA für das EPA sind die Räumlichkeiten von Getronics PinkRoccade (GPR) in Apeldoorn. Alle Arbeiten zum Betrieb der CA für das EPA sowie zur Verarbeitung von Smartcards für das EPA werden in der hierfür vorgesehenen, physikalisch geschützten Umgebung bei GPR durchgeführt.

Die CA für das EPA verfügt über maximal sechs physikalische Sicherheitsschichten. Sie sind in Abschnitt 5.1.2 beschrieben und setzen sich zusammen wie folgt:

- Ausstellung von Smartcards (Schicht 3)
- CA-Funktionen (Schicht 4)
- Online zu betreibende kryptografische Module für die CA für das EPA (Schicht 5)
- Offline zu betreibende kryptografische Module für die CA für die Europäische Patentorganisation (Schicht 7)

Die CA für das EPA wählt für ihren Betriebsort geschützte Räumlichkeiten, deren Innen und/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).

Betriebsort der RA für das EPA sind die eBusiness-Nutzerunterstützung-Räumlichkeiten in Dienstort München, wo auch die Validierung erfolgt.

### 5.1.2. Physikalischer Zugang

Informationsträger mit Angaben zum physikalischen Zugang sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.
Der physikalische Zugang zur CA für das EPA ist folgendermaßen gekennzeichnet:

- Der Zugang zu Schicht 1 bei GPR erfordert einen Mitarbeiterausweis in Form einer berührungslos lesbaren Chipkarte.

- Für den Zugang zu Schicht 2 ist eine Einzelkontrolle aller Personen erforderlich, die die allgemein genutzten Bereiche der CA für das EPA betreten wollen und sich dabei über einen Mitarbeiterausweis in Form einer berührungslos lesbaren Chipkarte ausweisen müssen.
- Für den Zugang zu Schicht 3 ist eine Einzelkontrolle erforderlich, bei der zwei Faktoren einschließlich Biometriedaten überprüft werden.
- Für den Zugang zum Datenzentrum der Schicht 4 ist eine Einzelkontrolle erforderlich, und der Raum, wo die Schlüsselvergabe erfolgt, ist nach einer zweifachen Kontrolle von jeweils zwei Faktoren einschließlich Biometriedaten zugänglich.
- Schicht 5-7: Online betriebene kryptografische Sicherheitseinheiten (CSUs) sind durch die Verwendung abschließbarer Schränke geschützt. Offline betriebene CSUs sind durch die Verwendung abschließbarer Safes, Schränke und Behältnisse geschützt. Der Zugang zu den CSUs sowie zu Schlüsselmaterial ist entsprechend den Anforderungen hinsichtlich der Aufgabentrennung bei GPR beschränkt.
- Der physikalische Zugang zu den vorstehend beschriebenen Schichten wird in jedem Fall automatisch protokolliert.

Der physikalische Zugang zur RA für das EPA ist folgendermaßen gekennzeichnet:

- Die Abteilung eBusiness-Nutzerunterstützung des EPA wird von Sicherheitspersonal bewacht.
- Die Abteilung eBusiness-Nutzerunterstützung des EPA steht den EPA-Bediensteten während der Dienstzeiten offen.
- Außerhalb der Dienstzeiten ist die Abteilung eBusiness-Nutzerunterstützung geschlossen.
- Alle Daten der RA für das EPA werden durch die Verwendung abschließbarer Schränke geschützt.

### 5.1.3. Stromversorgung und Klimatisierung

Die sicherheitsrelevanten Einrichtungen von CA und RA für das EPA sind mit folgenden Systemen ausgestattet, und zwar jeweils für die Primär-und Notversorgung:

- Stromversorgungssysteme, die den unterbrechungsfreien Zugang zu elektrischem Strom gewährleisten
- Heizungs-/Belüftungs-/Klimaanlagen zur Regelung von Temperatur und relativer Feuchte

### 5.1.4. Schutz vor Wasserschäden

Die CA für das EPA ergreift geeignete Maßnahmen zum Schutz vor Überschwemmungen im Betriebsgebäudeinneren, die durch Wassereinbruch von außen oder auch durch auslaufendes Kühlwasser und/oder Heizungsanlagen verursacht werden und wichtige Betriebsabläufe beeinträchtigen könnten (Auswahl eines geografischen Standorts über dem Meeresspiegel).

### 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

Informationsträger mit Angaben zur Lagerung von Datenträgern sind gesondert

aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Die CA für das EPA lagert ihre auswechselbaren Datenträger im EPA/bei GPR oder an einem sicheren Ort außerhalb.

#### 5.1.7. Abfallentsorgung

Informationsträger mit Angaben zur Abfallentsorgung sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Vertrauliche Dokumente und Materialien werden vor der Entsorgung im Reißwolf zerkleinert. Kryptografische Geräte werden gemäß den Entsorgungsrichtlinien des Herstellers physikalisch zerstört oder auf Null zurückgesetzt. Sonstiger Abfall wird entsprechend den normalen Abfallentsorgungsbestimmungen von EPA und GPR entsorgt.

#### 5.1.8. Externe Datensicherung

CA und RA für das EPA stellen sicher, dass wichtige Systemdaten, Prüfprotokolldaten und andere vertrauliche Daten regelmäßig extern gesichert werden.

### 5.2. Verfahrenskontrollen

#### 5.2.1. Vertrauenspositionen

Informationsträger mit Angaben zu Vertrauenspositionen sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Zu den Vertrauenspersonen zählen alle Mitarbeiter, Vertragsmitarbeiter und Berater von GPR und EPA mit Zugang zu oder Kontrolle über Authentifizierungs-oder kryptografische Operationen, die folgende Vorgänge erheblich beeinträchtigen können:

- Validierung von Angaben in Zertifikatanträgen
- Annahme, Ablehnung oder sonstige Bearbeitung von Zertifikatanträgen, Sperranträgen, Erneuerungsanträgen oder Registrierungsdaten
- Ausstellung oder Sperrung von Zertifikaten; dies gilt auch für Personal mit Zugang zu Verzeichnisbereichen, die der Geheimhaltung unterliegen
- Weiterleitung von Daten oder Anträgen des Zertifikatnehmers

Zu den Vertrauenspersonen gehören u.a.:

- Kundendienstpersonal
- Personal zur Durchführung kryptografischer Geschäftsvorgänge
- Sicherheitspersonal
- Systemverwaltungspersonal
- spezielles technisches Personal
- Führungskräfte, die die Vertrauenswürdigkeit der Infrastruktur sicherstellen sollen

Personen, die durch Übernahme einer Vertrauensposition den Status einer Vertrauensperson erlangen möchten, müssen die nachfolgend beschriebenen Prüfkriterien erfüllen. Alle Mitarbeiter haben eine Sicherheitserklärung zu unterzeichnen.

### 5.2.2. Anzahl der Bearbeiter je Aufgabe

Informationsträger mit Angaben zur Anzahl der erforderlichen Bearbeiter je Aufgabe sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Aufgaben, die innerhalb der CA für das EPA als besonders sicherheitskritisch anzusehen sind, z. B. der Zugang zu und die Verwaltung von kryptografischen Modulen der CA für das EPA und den entsprechenden Schlüsselmaterialien, sind immer von mindestens zwei Vertrauenspersonen auszuführen.

Die RA-Funktion bei der RA für das EPA erfüllt ein Mitarbeiter, der Zertifikatanträge, Sperrund Erneuerungsanträge sowie Registrierungsdaten bearbeitet.

## 5.3. Kontrolle des Personals

### 5.3.1. Erfordernisse hinsichtlich Hintergrund, Qualifikationen, Erfahrungen und Sicherheitsüberprüfung

Informationsträger mit Angaben zu den Erfordernissen hinsichtlich Hintergrund, Qualifikationen, Erfahrungen und Sicherheitsüberprüfung sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Mitarbeiter, die den Status einer Vertrauensperson erlangen möchten, müssen nachweisen, dass sie über den Hintergrund, die Qualifikationen und Erfahrungen verfügen, die erforderlich sind, um die Tätigkeit verantwortungsvoll und zufrieden stellend ausüben zu können.

### 5.3.2. Verfahren zur Überprüfung des Hintergrunds

Informationsträger mit Angaben über Verfahren zur Überprüfung des Hintergrunds sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.
Vor der Anstellung in einer Vertrauensposition führt die CA für das EPA eine Überprüfung des Hintergrunds durch, die Folgendes beinhaltet:

- Bestätigung des vorherigen Beschäftigungsverhältnisses
- Überprüfung der beruflichen Referenzen
- Bestätigung des höchsten oder wichtigsten Bildungsgrads, der erreicht wurde
- Überprüfung des Hintergrunds

Bei der Überprüfung des Hintergrunds können sich Faktoren ergeben, die als Grund für die Ablehnung eines Bewerbers um eine Vertrauensposition gelten können. Dies sind u. a.:

- falsche Angaben des Bewerbers
- äußerst ungünstige oder unzuverlässige persönliche Referenzen
- gewisse Vorstrafen

### 5.3.3. Erfordernisse hinsichtlich der Schulung

Unterstützungspersonal für die EPA-PKI wird nach der Einstellung geschult und erhält zusätzlich die notwendige arbeitsbegleitende Ausbildung, die erforderlich ist, um die jeweiligen Aufgaben kompetent und zufrieden stellend erledigen zu können.

Ausbildungsprogramme beinhalten:

- PKI-Grundlagen
- Mit der jeweiligen Funktion verbundene Aufgaben
- Richtlinien und Verfahren für Sicherheit und Betrieb
- Einsatz und Betrieb der installierten Hardware und Software
- Meldung und Vorgehensweise bei besonderen Vorkommnissen und im Kompromittierungsfall
- Verfahren zur Wiederherstellung im Katastrophenfall und zur Aufrechterhaltung der Geschäftsprozesse

### 5.3.4. Häufigkeit von Nachschulungen und Erfordernisse

Das Personal erhält Schulungen zur Auffrischung der Kenntnisse. Es werden laufend Sicherheitsschulungen abgehalten, an denen das Personal regelmäßig teilzunehmen hat.

### 5.3.5. Häufigkeit und Reihenfolge beim regelmäßigen Tätigkeitswechsel

Informationsträger mit Angaben zur Häufigkeit und Reihenfolge beim regelmäßigen Tätigkeitswechsel sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

### 5.3.6. Disziplinarmaßnahmen bei unerlaubten Handlungen

Mitarbeiter, die gegen die Bestimmungen der CP, der CPS oder andere Richtlinien und Verfahren verstoßen, haben Disziplinarmaßnahmen von der CA für die EPA zu erwarten. Je nach Häufigkeit und Schwere der Verstöße können Disziplinarmaßnahmen bis hin zur Entlassung ergriffen werden.

### 5.3.7. Erfordernisse im Hinblick auf Vertragspersonal

Informationsträger mit Angaben zu Erfordernissen im Hinblick auf Vertragspersonal sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

In Ausnahmefällen können unabhängige Vertragsmitarbeiter oder Berater eingesetzt werden, um Vertrauenspositionen zu besetzen. Für Vertragsmitarbeiter und Berater gelten die gleichen funktionellen und Sicherheitsanforderungen wie für EPA-und GPR-Personal.

### 5.3.8. Unterlagen für das Personal

Alle bei der RA für das EPA und der CA für das EPA tätigen Mitarbeiter sind verpflichtet, diese CPS, die CP für das EPA und die geltenden Sicherheitsrichtlinien zu lesen.

## 6. TECHNISCHE SICHERHEITSKONTROLLEN

Die CA für das EPA ist der CA für die Europäische Patentorganisation nachgeordnet (siehe auch 1.3.1). Dieses Kapitel beschreibt die Sicherheitskontrollen zum Schutz der CA für das

EPA sowie der von ihr ausgegebenen Teilnehmerschlüssel.

## 6.1. Erzeugung und Installation von Schlüsselpaaren

### 6.1.1. Erzeugung von Schlüsselpaaren

Informationsträger mit Angaben zur Erzeugung von Schlüsselpaaren sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Die CA für das EPA und die CA für die Europäische Patentorganisation verwenden eigenständige hardwarebasierte kryptografische Module, welche in Bezug auf die Erzeugung von Schlüsselpaaren zur Signierung und Verifizierung von Zertifikaten den Standard FIPS PUB 140-1 bis zur Sicherheitsstufe 3 erfüllen und entsprechend zertifiziert sind.

Die RA für das EPA erzeugt ihre Schlüsselpaare mit Hilfe eines kryptografischen Moduls, das gemäß FIPS 140-1, Stufe 1 zertifiziert und in der eingesetzten Browser-Software enthalten ist.

Teilnehmerschlüsselpaare werden direkt auf der Teilnehmer-Smartcard erzeugt. Infolgedessen bleiben die Schlüssel immer Bestandteil der Karte. Die Karte selbst ist mit einer PIN geschützt, die nur der Zertifikatnehmer kennt.

### 6.1.2. Auslieferung privater Schlüssel an Entitäten

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

### 6.1.3. Auslieferung öffentlicher Schlüssel an Zertifikatausssteller

Informationsträger mit Angaben zur Auslieferung öffentlicher Schlüssel an Zertifikatausssteller sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Öffentliche Teilnehmerschlüssel werden von der CA für das EPA direkt auf der Teilnehmer-Smartcard erzeugt. Für jedes Zertifikat erzeugt das Smartcard-Managementsystem (CMS) einen Zertifikatantrag gemäß PKCS#10 und schickt ihn zur Bearbeitung an die CA für das EPA. Nach Eingang einer Rückmeldung der CA für das EPA gemäß PKCS#7 speichert das Smartcard-Managementsystem das Zertifikat auf der Teilnehmer-Smartcard ab. Sobald das Zertifikat auf der Smartcard gespeichert ist, wird für die Teilnehmer-PIN ein Zufallswert ausgewählt. Diese PIN schickt GPR dann gemäß Abschnitt 4.3 per E-Mail an den Zertifikatnehmer.

### 6.1.4. Auslieferung des öffentlichen Schlüssels der CAfür das EPA sowie der Sperrliste an berechtigte Nutzer

Der öffentliche Schlüssel der CA für das EPA steht berechtigten Nutzern zur Verfügung und wird als selbst unterzeichnetes Zertifikat (Self-signed Certificate) auf der CD mitgeliefert. Die Sperrliste wird von Getronics PinkRoccade unter http://www.megasign.nl/crl/EuropeanPatentOfficeepoline/LatestCRL.crl veröffentlicht.

### 6.1.5. Schlüsselumfang

Die Schlüssel der CA für das EPA weisen eine Länge von 2 048 Bit auf.
Teilnehmerschlüssel weisen eine Länge von 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, das den Standard FIPS PUB 140-1, Stufe 3 erfüllt.
Teilnehmerschlüssel werden direkt auf der Smartcard des Nutzers erzeugt.

### 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, das in Bezug auf den Schutz ihres privaten Schlüssels den Standard FIPS PUB 140-1, Sicherheitsstufe 3 erfüllt und entsprechend zertifiziert ist.
Der private Teilnehmerschlüssel ist auf einer Smartcard gemäß FIPS PUB 140-1 gespeichert.

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

Informationsträger mit Angaben zur Kontrolle privater Schlüssel durch mehrere (n von m) Personen sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Die CA für das EPA hat technische und verfahrenstechnische Mechanismen implementiert, die es erfordern, dass sicherheitsempfindliche kryptografische Operationen der CA immer in Anwesenheit mehrerer vertrauenswürdiger Person durchgeführt werden. Um den auf diesem Modul gespeicherten privaten Schlüssel der CA für das EPA zu aktivieren, sind mindestens drei von insgesamt neun Schlüsseln erforderlich, die für das kryptografische Modul der CA für das EPA erzeugt und verteilt wurden.

Der Teilnehmerschlüssel ist auf einer Smartcard gespeichert, und die Karte selbst ist durch eine nur dem Zertifikatnehmer bekannte PIN geschützt.

### 6.2.3. Hinterlegung privater Schlüssel bei Dritten

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

### 6.2.4. Sicherung privater Schlüssel

Im Hinblick auf die routinemäßige Wiederherstellung sowie die Wiederherstellung im

Katastrophenfall fertigt die CA für das EPA Sicherungskopien ihrer privaten Schlüssel an. Diese Schlüssel werden in verschlüsselter Form in kryptografischen Modulen und damit verbundenen Schlüsselspeichern gespeichert.

Die CA für das EPA sichert keine privaten Schlüssel der RA für das EPA oder der Zertifikatnehmer.

### 6.2.5. Archivierung privater Schlüssel

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

Die CA für das EPA sichert keine privaten RA-oder Teilnehmerschlüssel.

### 6.2.6. Transfer privater Schlüssel in das kryptografische Modul der CAfür das EPA

Informationsträger mit Angaben zum Transfer privater Schlüssel in das kryptografische Modul der CA für das EPA sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

CA-Schlüsselpaare erzeugt die CA für das EPA auf dem Hardwaremodul, auf dem die Schlüssel verwendet werden. Im Hinblick auf die routinemäßige Wiederherstellung sowie die Herstellung im Katastrophenfall fertigt die CA für das EPA zudem Sicherheitskopien dieser Schlüssel an. In Fällen, wo die Datensicherung auf einem anderen kryptografischen Hardwaremodul erfolgt, werden die Schlüsselpaare in verschlüsselter Form von einem Modul zum anderen übertragen.

### 6.2.7. Verfahren zur Aktivierung privater Schlüssel

Informationsträger mit Angaben über das Verfahren zur Aktivierung privater Schlüssel sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Der private Schlüssel der CA für die Europäische Patentorganisation wird nur aktiviert, um das Zertifikat der CA für das EPA zu signieren, danach wird er deaktiviert und das Sicherheitsmodul wird wieder an einem sicheren Ort verwahrt.
Die privaten Schlüssel des Administrators der RA für das EPA sind auf einer Smartcard gespeichert und werden über einen dem Administrator bekannten PIN-Code aktiviert.

Teilnehmerschlüsselpaare werden direkt auf der Smartcard des Zertifikatnehmers erzeugt. Infolgedessen bleiben die Schlüssel immer Bestandteil der Karte. Die privaten Teilnehmerschlüssel werden über einen PIN-Code aktiviert, der nur dem Zertifikatnehmer bekannt ist.

### 6.2.8. Verfahren zur Deaktivierung privater Schlüssel

Die privaten Schlüssel des Administrators der RA für das EPA werden bei Abmeldung aus dem System deaktiviert. Der RA-Administrator muss sich abmelden, bevor er den Arbeitsplatz verlässt.

Private Teilnehmerschlüssel werden beim Entfernen der Smartcard aus dem Lesegerät deaktiviert.

### 6.2.9. Verfahren zur Vernichtung privater Schlüssel

Die CA für das EPA deaktiviert ihren privaten Schlüssel, indem sie ihn unwiderruflich vernichtet.

Die Vernichtung von Teilnehmerschlüsseln ist nicht möglich, aber das jeweilige Zertifikat kann gesperrt werden, um den Missbrauch eines privaten Schlüssels zu verhindern (siehe 4.4.1). Die Ersatzkarte enthält neue Schlüssel und Zertifikate.

## 6.3. Sonstige Aspekte der Verwaltung von Schlüsselpaaren

### 6.3.1. Archivierung öffentlicher Schlüssel

Das Zertifikat der CA für das EPA, das Zertifikat der RA für das EPA sowie die Teilnehmerzertifikate werden im Rahmen der routinemäßigen Datensicherung der CA für das EPA gesichert und archiviert.

### 6.3.2. Geltungsdauer 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

Informationsträger mit Angaben zur Erzeugung und Installation von Aktivierungsdaten sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

Zum Schutz privater Schlüssel verwendet die CA für das EPA starke Passwörter. Entsprechend den Auswahlrichtlinien sollten Passwörter

- vom Nutzer erzeugt werden,
- aus mindestens acht Zeichen bestehen,
- mindestens ein alphabetisches und ein numerisches Zeichen enthalten,
- mindestens ein kleingeschriebenes Zeichen enthalten,
- ein und dasselbe Zeichen nicht zu oft enthalten,
- nicht mit dem Profilnamen des Nutzers übereinstimmen,
- keine langen Teilzeichenfolgen aus dem Profilnamen des Nutzers enthalten.

Zur Aktivierung privater Schlüssel wendet die RA für das EPA starke Authentifizierungskriterien an: Smartcard und PIN-Code.

Auch Zertifikatnehmer wenden zur Aktivierung privater Schlüssel starke Authentifizierungskriterien an: Smartcard und PIN-Code (siehe auch 6.1.3).

### 6.4.2. Schutz von Aktivierungsdaten

Administratoren der CA für das EPA müssen ihre Schlüssel sicher aufbewahren und eine Verpflichtungserklärung unterschreiben.

Administratoren der RA für das EPA müssen die privaten Administratorenschlüssel in verschlüsselter Form auf einer Smartcard speichern.

### 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

RA und CA für das EPA führen Kontrollen zur Computersicherheit durch, umden einzelnen Mitarbeiter zu identifizieren. Der Zugang zur Hardware der RA für das EPA sowie zur CMS-Hardware erfolgt über Smartcard und PIN. Darüber hinaus begrenzt die CA für das EPA den Zugang zu Daten und Funktionen entsprechend der Funktion und den Rechten des Nutzers und hält jeden Zugriff in einem Online-Protokoll (Prozesshistorie) für sicherheitsrelevante Ereignisse fest.

### 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. Kontrolle des Sicherheitsmanagements

Die CA für das EPA baut ein Sicherheitssystem auf und verwaltet und kontrolliert alle Sicherheitsmaßnahmen im Hinblick auf Systementwicklung und –betrieb.

### 6.6.3. Sicherheitseinstufung während der Lebensdauer

Nicht zutreffend.

## 6.7. Kontrolle der Netzsicherheit

Informationsträger mit Angaben zur Kontrolle der Netzsicherheit sind gesondert aufzubewahren. Aus Sicherheitsgründen dürfen diese Informationen nicht öffentlich bekannt gemacht werden. Zugang zu diesen Informationen können berechtigte Personen erhalten, wenn beim Direktorat Sicherheit und Audit des EPA ein begründeter Antrag gestellt wurde.

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. Jede Firewall wird entsprechend den jeweiligen Sicherheitsvorgaben so konfiguriert, dass der Datenverkehr zwischen den Netzen auf ein Maß begrenzt wird, das zur Erreichung der Geschäftsziele unbedingt erforderlich ist; außerdem werden eingehende Daten gegebenenfalls auf Virenbefall überprüft. Die Firewalls werden regelmäßigen und speziellen Kontrollen unterzogen, um tatsächliche oder mutmaßliche Sicherheitsverstöße zu erkennen.

Zwischen RA für das EPA und CMS (Smartcard-Managementsystem) werden die Daten verschlüsselt übertragen, und beide Systeme müssen sich voreinander authentifizieren.

Alle zwischen dem CMS-Registrierungsbaustein und der CA für das EPA ausgetauschten Daten werden digital signiert. Zu diesem Zweck verwendet der CMS-Server

- ein eindeutiges Zertifikat der RA für das EPA mit dazu passendem Schlüssel,
- das öffentliche Zertifikat der CA für das EPA.

Alle Antragsvorgänge werden unter Verwendung des Zertifikats der RA für das EPA digital signiert. So kann die CA für das EPA erkennen, dass sie nur von einer registrierten RA für das EPA stammen können.

Alle Antworten der CA für das EPA an die RA für das EPA werden mit dem privaten Schlüssel der CA für das EPA signiert. So kann das CMS erkennen, dass sie tatsächlich von der CA für das EPA stammen.

### 6.8. Kontrolle der technischen Ausführung des kryptografischen Moduls

Siehe Abschnitt 6.2.1.

# 7. PROFIL VON ZERTIFIKATEN UND SPERRLISTEN

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

## 7.1. Zertifikatprofil

Teilnehmerzertifikate entsprechen den Anforderungen gemäß RFC 2459. Das Zertifikatprofil enthält folgende Werte oder Werteinschränkungen:

| Feld | Wert oder Werteinschränkung |
|---|---|
| Version | Siehe CPS § 7.1.1 |
| Serial number | Eindeutiger Wert für jeden DN (MD5-Hash des öffentlichen Schlüssels) |
| Signature algorithm | SHA1 RSA |
| Issuer DN | Siehe Abschnitt 7.1.4. |
| Valid from | Ausstellungsdatum (basierend auf Coordinated Universal Time (UTC), codiert gemäß RFC 2459). |
| Valid to | Ausstellungsdatum + 3 Jahre (basierend auf UTC, codiert gemäß RFC 2459). |
| Subject DN | C: Land des Zertifikatnehmers |
| | O: Firma des Zertifikatnehmers |
| | CN: <Erster Buchstabe des Vornamens> + <.>+ <-> +<Erster Buchstabe des zweiten Vornamens> + <Leer> + <Nachname> + <Leer> + <EPA ID> |
| Subject public key | Codiert entsprechend RFC 2459 unter Verwendung von Algorithmen gemäß CPS, Abschnitt 7.1.3 und Schlüssellängen gemäß CPS, Abschnitt 6.1.5. |
| Signature | Erzeugt und codiert gemäß RFC 2459. |

**Tabelle 2 Zertifikatprofil**

### 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 hat eine einzige nicht kritische, CP-bezogene Zertifikaterweiterung gemäß RFC 2459 implementiert, wobei jedes Zertifikat so genannte CP-Qualifier enthält.

### 7.1.3. Object Identifier für Algorithmen

Teilnehmerzertifikate werden gemäß RFC 2459 mit SHA-1 und RSA-Verschlüsselung (1 2 840 113549 1 1 5) signiert.

### 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

Das Sperrlistenprofil enthält die nachfolgend aufgeführten Basisfelder und Feldinhalte:

| Feld | Wert oder Werteinschränkung |
|---|---|
| Version | Siehe CPS, Abschnitt 7.2.1 |
| Signature algorithm | Md5RSA oder md2RSA |
| Issuer | Ersteller der Sperrliste. Der Name des Erstellers entspricht dem in 7.1.4 angegebenen Format. |
| Effective date | Ausgabedatum der Sperrliste. |
| Next update | Datum für die nächste Sperrlistenausgabe. Die nächste Aktualisierung erfolgt drei Monate nach dem Ausgabedatum der Sperrliste für die CA für die Europäische Patentorganisation. Sperrlisten für Teilnehmerzertifikate werden in regelmäßigen Abständen gemäß CPS, Abschnitt 4.4.9 herausgegeben. |
| Revoked certificates | Auflistung gesperrter Zertifikate, einschließlich Seriennummer und Sperrdatum des gesperrten Zertifikats |
| Signature | Erzeugt und codiert gemäß RFC 2459. |

**Tabelle 3 Basisfelder des Sperrlistenprofils**

### 7.2.1. Versionsnummer(n)

Die CA für das EPA gibt Sperrlisten gemäß X.509, Version 1 heraus.

### 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.