Erklärung zum Zertifizierungsbetrieb der obersten Zertifizierungsstelle der Public Key Infrastruktur im Deutschen Forschungsnetz

- Classic -

DFN-Verein

CPS-Classic V1.1, Februar 2005

Inhaltsverzeichnis

1 Einleitung

Der Verein zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN-Verein) betreibt das Deutsche Forschungsnetz (DFN) und stellt seine Weiterentwicklung und Nutzung sicher. Dieses Hochleistungsnetz für Wissenschaft und Forschung verbindet Hochschulen und Forschungseinrichtungen miteinander und unterstützt die Entwicklung und Erprobung neuer Anwendungen in Deutschland. Auf dieser Basis stellt der DFN-Verein Dienste zur Verfügung. Einer dieser Dienste ist die Bereitstellung einer Public Key Infrastruktur (PKI), die u.a. für Nutzer, Datenverarbeitungssysteme (Rechner, Dienste, Anwendungen, Prozesse) und nachgeordnete Zertifizierungsdienste Zertifikate ausstellt.

Die Public Key Infrastruktur im Deutschen Forschungsnetz (DFN-PKI) unterstützt verschiedene Klassen von Zertifizierungsdienstleistungen, wobei jede Klasse unterschiedliche Sicherheitsanforderungen besitzen und spezifische Funktionen aufweisen kann. Teilnehmer an der DFN-PKI können eine Zertifikatklasse mit bestimmten Eigenschaften entsprechend ihren Anforderungen, auswählen. Je nach gewünschter Zertifikatklasse kann ein Zertifikat entweder elektronisch, schriftlich oder persönlich bei einer Registrierungsstelle durch einen Teilnehmer beantragt werden. Jedes ausgestellte Zertifikat entspricht, abhängig von der gewählten Klasse, einem spezifischen Sicherheitsniveau innerhalb der DFN-PKI.

Es können innerhalb der DFN-PKI verschiedene Zertifizierungsstellen existieren, die Zertifikate für die jeweiligen Sicherheitsniveaus ausstellen, wobei sich die jeweils erbrachten Dienstleistungen voneinander in Art und Weise der Erbringung sowie verfügbarer Mehrwerte unterscheiden können. Auch die jeweils angewandten Verfahren können unterschiedlich sein, sofern diese der Zertifizierungsrichtlinie und der Erklärung zum Zertifizierungsbetrieb der DFN-PKI entsprechen. Eine Darstellung der verschiedenen Betriebsmodelle innerhalb der Zertifizierungshierarchie ist der Abbildung 1 zu entnehmen. Somit kann jede Organisation in dem eingeräumten Rahmen Verfahren etablieren bzw. anpassen, um ihren spezifischen Anforderungen gerecht zu werden.

1.1 Überblick

Dieses Dokument enthält die Erklärung zum Zertifizierungsbetrieb (Certificate Practice Statement, CPS) der DFN-PKI. Diesem Dokument zugehörig ist eine Zertifizierungsrichtlinie (Certification Policy, CP).

CPS und CP berücksichtigen die Anforderungen aus RFC 3647 [RFC 3647].

Um die internationale Zusammenarbeit mit anderen Zertifizierungsstellen zu ermöglichen, wird ferner eine englische Übersetzung von CPS und CP veröffentlicht; maßgeblich ist in jedem Fall die deutsche Version in der aktuellen Fassung.

Im Folgenden steht der Begriff DFN-PKI für den Teil der gesamten DFN-PKI, die dem hier definierten Sicherheitsniveau Classic unterliegt.

In diesem CPS der DFN-PKI sind detaillierte Informationen über Spezifikationen, über Prozesse der Zertifizierungsstelle und über technische Sicherheitsmaßnahmen für die Ausstellung von Zertifikaten - entsprechend der internationalen Norm X.509 [X.509] - für das Sicherheitsniveau Classic enthalten.

Die Eigenschaften der Zertifikate und Vorgaben für das jeweilige Sicherheitsniveau sind der entsprechenden CP [CP-Classic] zu entnehmen. Für das genannte Sicherheitsniveau werden Zertifikate ausschließlich auf Basis dieser CP ausgestellt, die getroffenen Aussagen sind für alle Teilnehmer bindend, soweit sie nicht gesetzlichen Regelungen widersprechen.

Der Betrieb der obersten Zertifizierungsstelle (Policy Certification Authority, PCA) für das Deutsche Forschungsnetz, der Betrieb von Zertifizierungsstellen für DFN-Anwender, der Betrieb zentraler Zertifizierungsstellen für einzelne Nutzer, deren Organisationen bisher keine

eigenen Zertifizierungsdienstleistungen anbieten, sowie die Koordinierung und Abstimmung mit den innerhalb der DFN-PKI operierenden Zertifizierungsstellen erfolgt im Auftrag des DFN-Vereins durch den Dienstleister DFN-CERT Services GmbH (Kontakt siehe Abschnitt 1.5.1).

1.2 Identifikation des Dokuments

Identifikation

- **Titel: Erklärung zum Zertifizierungsbetrieb der Public Key Infrastruktur im Deutschen Forschungsnetz - Classic -**
- **Version: 1.1**
- **Object Identifier (OID): 1.3.6.1.4.1.22177.300.2.1.1.1.1**
- **Zusammensetzung der OID:**

IANA	**1.3.6.1.4.1**
DFN-Verein	**22177**
PKI	**300**
Erklärungen zum Zertifizierungsbetrieb	**2**
X.509	**1**
Classic	**1**
Hauptversion	**1**
Nebenversion	**1**

1.3 Teilnehmer der Zertifizierungsinfrastruktur

1.3.1 Zertifizierungsstellen

1.3.1.1 Oberste Zertifizierungsstelle (PCA)

Der öffentliche Schlüssel (Public Key) der obersten Zertifizierungsstelle ist in einem selbstsignierten Zertifikat (Wurzel-Zertifikat) enthalten. Alle Teilnehmer der DFN-PKI erhalten das Zertifikat und können somit die Authentizität und Gültigkeit aller unterhalb dieses Wurzelzertifikates innerhalb der DFN-PKI ausgestellten Zertifikate überprüfen.

Die PCA zertifiziert ausschließlich Zertifikate von unmittelbar nachgeordneten Zertifizierungsstellen.

1.3.1.2 Zertifizierungsstellen (CA)

Unterhalb der unmittelbar der PCA nachgeordneten Zertifizierungsstelle „CA-Services“ werden folgende Zertifizierungsstellen betrieben:

- **User-CA,**
  Zertifizierungsstelle für natürliche Personen und Personengruppen
- **Server-CA,**
  Zertifizierungsstelle für Datenverarbeitungssysteme
- **Object-Signing-CA,**
  Zertifizierungsstelle für Software-Hersteller

Diese Zertifizierungsstellen stellen Zertifikate für einzelne Nutzer aus, deren Organisationen bisher keine eigenen Zertifizierungsdienstleistungen anbieten. Es werden keine Zertifikate für weitere, nachgeordnete Zertifizierungsstellen ausgestellt.

1.3.2 Registrierungsstellen

Die ausgezeichneten Registrierungsstellen für die zuvor genannten Zertifizierungsstellen befinden sich in den Räumen der DFN-CERT Services GmbH. Darüber hinaus sind die folgenden Registrierungsstellen verfügbar:

- **DFN-Verein, Geschäftsstelle Berlin**
- **DFN-Verein, Geschäftsstelle Stuttgart**

Die vollständige Liste aller Registrierungsstellen wird über den in Abschnitt 2.2 genannten Web-Server veröffentlicht.

Die Identitätsprüfung von Zertifikatnehmern kann von Mitarbeitern der Registrierungsstellen auch außerhalb der Betriebsräume vorgenommen werden.

1.3.3 Zertifikatnehmer

Die Vergaberegelung hängt von der Zertifikatklasse ab und wird in der zugehörigen CP geregelt.

1.3.4 Zertifikatprüfer

Aussagen über Zertifikatprüfer sind der zugehörigen CP zu entnehmen.

1.3.5 Weitere Teilnehmer

Entfällt.

1.4 Anwendungsbereich

Der genaue Anwendungsbereich wird in der zugehörigen CP geregelt.

1.5 Verwaltung der Richtlinien

1.5.1 Organisation

Die Verwaltung der Richtlinien erfolgt durch:

DFN-Verein	**Telefon: +49 30 884299-24**
Stresemannstr. 78	**Telefax: +49 30 884299-70**
	E-Mail: pki@dfn.de
D - 10963 Berlin	**WWW: http://www.dfn.de/pki**

Der Betrieb der unter Abschnitt 1.3. aufgeführten Zertifizierungsstellen erfolgt durch:

DFN-CERT Services GmbH	**Telefon: +49 40 808077-555**
DFN-PCA	**Telefax: +49 40 808077-556**
Heidenkampsweg 41	**E-Mail: certify@pca.dfn.de**
D - 20097 Hamburg	**WWW: https://www.pca.dfn.de**

1.5.2 Kontaktperson

Die verantwortliche Person für die CP ist:

DFN-Verein	**Telefon: +49 30 884299-24**
Dr. Marcus Pattloch	**Telefax: +49 30 884299-70**
Stresemannstr. 78	**E-Mail: pattloch@dfn.de**
D - 10963 Berlin	**WWW: http://www.dfn.de/pki**

1.5.3 Verantwortliche Person für das CPS

Die in Abschnitt 1.5.2 genannte Person ist auch verantwortlich für das CPS.

1.5.4 Genehmigungsverfahren

Die Genehmigung der CP und des CPS erfolgt durch die in Abschnitt 1.5.2 genannte verantwortliche Person, ein spezielles Genehmigungsverfahren gibt es nicht.

1.5.5 Änderungen der Richtlinien

Änderungen an den Richtlinien können jederzeit unter den im Abschnitt 1.5.4. beschriebenen Verfahren vorgenommen werden.

Werden Änderungen vorgenommen, die sicherheitsrelevante Aspekte betreffen oder die Abläufe seitens der Zertifikatnehmer erforderlich machen, ist eine Änderung der OID des entsprechenden Dokuments erforderlich.

Die geänderten Dokumente treten an dem Tag in Kraft, an dem sie über den in Abschnitt 2.2. beschriebenen Dienst veröffentlicht werden. Eine Änderung der CP wird in den DFN Mitteilungen angekündigt.

1.6 Definitionen und Abkürzungen

Siehe Glossar.

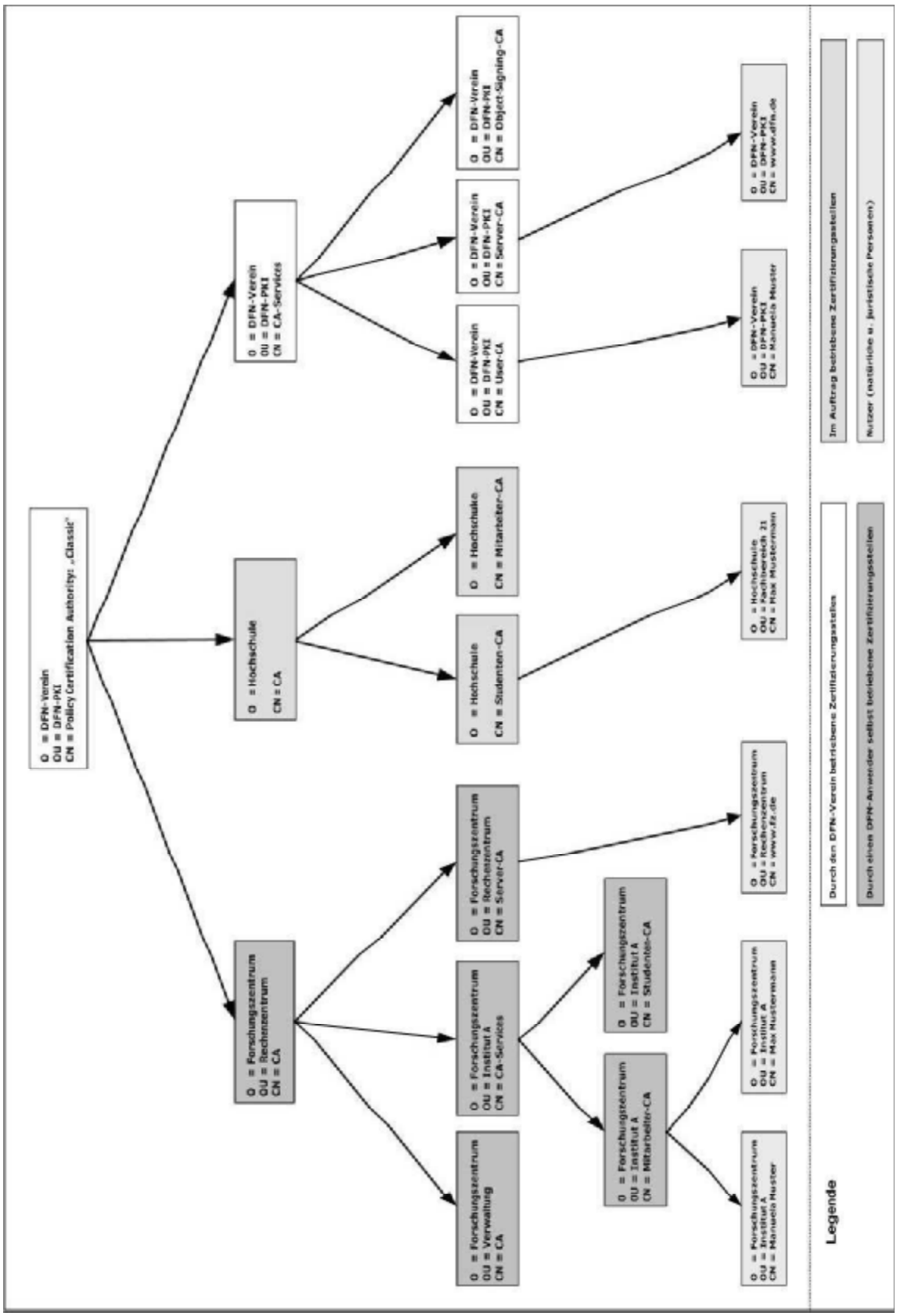

Abbildung 1: Zertifizierungshierarchie der DFN-PKI

2 Veröffentlichungen u. Verzeichnisdienst

2.1 Verzeichnisdienst

Der Verzeichnisdienst der PCA ist unter den folgenden Bezugsadressen online zu erreichen:

- **https://www.pca.dfn.de/dfn-pki/certification/cacert.html**
- **ldap://ldap1.pca.dfn.de/o=DFN-Verein/c=de???(objectclass=*)**

2.2 Veröffentlichung von Informationen

Die PCA publiziert die folgenden Informationen über https://www.pca.dfn.de:

- **Zertifikat und Fingerabdruck der PCA:**
  https://www.pca.dfn.de/dfn-pki/certification/x509/classic/g1/data/html/cacert.html
- **CP**
  https://www.pca.dfn.de/dfn-pki/certification/cp/classic/x509/
- **CPS**
  https://www.pca.dfn.de/dfn-pki/certification/cps/classic/x509/
- **Liste der Registrierungsstellen**
  https://www.pca.dfn.de/dfn-pki/certification/ra-list.html

2.3 Update der Informationen / Veröffentlichungsfrequenz

Neu ausgestellte Zertifikate, CRLs, Richtlinien und ggf. weitere Informationen werden zeitnah zur Verfügung gestellt. Es gelten die folgenden Veröffentlichungsfrequenzen:

- **Zertifikate:** **werden umgehend nach der Ausstellung eingestellt**
- **Widerrufslisten:** **mindestens einmal pro Monat**
- **Richtlinien:** **nach Bedarf**
- **Weitere Informationen:** **nach Bedarf**

2.4 Zugang zu den Informationsdiensten

Der lesende Zugriff auf alle in Abschnitt 2.1. und 2.2 aufgeführten Informationen unterliegt keiner Zugangskontrolle. Der schreibende Zugriff auf diese Informationen erfolgt ausschließlich durch berechtigte Mitarbeiter (siehe Abschnitt 5.2).

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensform

Die DNs aller Zertifikatnehmer unterhalb der PCA enthalten die Attribute „C=<Staat>“[1] und „O=<Organisation>“. Der Organisationsname enthält den Namen der Organisation, die der Zertifikatnehmer angehört und die im Fall einer Zertifizierungsstelle auch repräsentiert wird.

Der Name jedes Zertifikatnehmers der PCA entspricht grundsätzlich dem folgenden Schema:

C=DE,

O=<Organisation>,

[OU=<Organisationseinheit>,]

[CN=<Eindeutiger Name>,]

[EMAIL=<Email-Adresse>]

Das optionale Attribut „OU=<Organisationseinheit>“ kann mehrfach angegeben werden. Die Verwendung des Attributs "CN=" ist bei juristischen Personen nicht zwingend erforderlich, sollte jedoch aus Interoperabilitätsgründen verwendet werden. Für natürliche Personen ist dieses Attribut hingegen obligatorisch. Wenn eine E-Mail Adresse angegeben wird, so wird diese über das Attribut "EMAIL=" in den Namen aufgenommen. Weitere Attribute, die in den Namen aufgenommen werden können, sind dem Abschnitt 7.1 zu entnehmen.

3.1.2 Aussagekräftigkeit von Namen

Der Name muss den Zertifikatnehmer eindeutig identifizieren und in einer für Menschen verständlichen Form vorliegen. Bei der Namensvergabe gelten zusätzlich die folgenden Konventionen:

- **Datenverarbeitungssysteme**

  Der „common name“ eines Datenverarbeitungssystems sollte grundsätzlich den voll qualifizierten Domain-Namen, z.B.: „cn=ldap1.pca.dfn.de“ enthalten.
- **Externe Zertifikatnehmer, die nicht im Namen und Auftrag eines DFN-Anwenders handeln**

  Der „common name“ eines externen Zertifikatnehmers beginnt mit dem Kennzeichen „EXT:“, z.B.: „cn=EXT:Manuela Muster“.
- **Natürliche Personen**

  Namenszusätze können nur verwendet werden, wenn diese in einem amtlichen Ausweispapiers mit Lichtbild enthalten sind, z.B.: „cn=Max Mustermann, Dr.“.
- **Personen bzw. Funktionsgruppen**

  Der „common name“ einer Personen bzw. Funktionsgruppe beginnt mit dem Kennzeichen „GRP:“, z.B.: „cn=GRP:Poststelle“. Bei Zertifizierungs- und Registrierungsstellen kann darauf verzichtet werden, wenn die Funktion aus dem „common name“ erkenntlich ist.
- **Pseudonyme**

---

[1] ***Benutzt wird der ISO-Ländercode DIN EN ISO 3166-1.***

Der „common name“ eines Pseudonyms beginnt mit dem Kennzeichen „PN:“, z.B.: „cn=PN:Deckname“.

Die Zuordnung eindeutiger Seriennummern ist Abschnitt 7.1 zu entnehmen.

3.1.3 Pseudonymität / Anonymität

Es gelten die Regelungen aus Abschnitt 3.1.2. Die PCA und die CA-Services bieten diese Dienstleistungen nicht an.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Verwendete Zeichensätze und die Substitutionsregelungen für Sonderzeichen:

Erlaubte Zeichen sind: a-z A-Z 0-9 ' ( ) + , - . / : = ? Leerzeichen,

Substitutionsregeln:

Ä	**-->**	**Ae**
Ö	**-->**	**Oe**
Ü	**-->**	**Ue**
ä	**-->**	**ae**
ö	**-->**	**oe**
ü	**-->**	**ue**
ß	**-->**	**ss**

Andere Sonderbuchstaben mit Akzenten verlieren ihre jeweiligen Akzente. Ansonsten wird eine für das betreffende Zeichen gemeinhin verwendete Schreibweise aus den Zeichen a-z und A-Z so zusammengesetzt, dass der entsprechende Laut entsteht.

Zeichenkodierung ist PrintableString oder T61String (kein BMPString oder UTF8String) und IA5String für E-Mail Adressen.

3.1.5 Eindeutigkeit von Namen

Vorgaben zur Eindeutigkeit von Namen sind der zugehörigen CP zu entnehmen.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Erkennung, Authentifizierung und Funktion von Warenzeichen sind in der zugehörigen CP geregelt.

3.2 Identitätsüberprüfung bei Neuantrag

Die Regelungen sind der zugehörigen CP zu entnehmen.

3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Der Zertifikatnehmer muss bei der Zertifikatbeantragung versichern, dass er im Besitz des privaten Schlüssels ist. Folgendes Verfahren zur Überprüfung ist vorgesehen:

- **Schlüsselgenerierung durch den Zertifikatnehmer**

  Der Zertifikatnehmer erzeugt ein asymmetrisches, kryptographisches Schlüsselpaar unter Verwendung geeigneter Software (z.B. mit OpenSSL) und übermittelt anschließend die elektronisch signierte Zertifizierungsanfrage (Certificate Signing Request, CSR) an die zuständige RA. Die erfolgreiche Verifikation der Signatur des CSRs und der Nachweis seiner Authentizität ist eine Voraussetzung für die Zertifikatausstellung.

3.2.2 Authentifizierung einer Organisation

Die Authentifizierung einer Organisation erfolgt im Rahmen der Registrierung durch die Vorlage entsprechender Unterlagen. Zur Prüfung, ob eine Organisation zum Leistungsemp-

fang berechtigt ist, stellt der DFN-Verein der PCA eine entsprechende Liste zur Verfügung. Ansprechpartner beim DFN-Verein ist die in Abschnitt 1.5.2. genannte Person.

3.2.3 Authentifizierung einer natürlichen Person

Die grundlegenden Verfahren für die Identitätsprüfung einer natürlichen Person sind der entsprechenden CP zu entnehmen. Für die Authentifizierung einer natürlichen Person ist ein persönliches Treffen mit einem Mitarbeiter der in Abschnitt 1.3.2 aufgeführten Registrierungsstellen erforderlich.

Folgende Informationen werden benötigt:

- **Name, Vorname(n) und Namenszusätze soweit im Ausweispapier vermerkt**
- **Anschrift**
- **Art des Ausweispapiers, dessen Nummer u. ausstellende Behörde**

Zur Ausstellung eines Zertifikats werden darüber hinaus folgende Informationen benötigt:

- **E-Mail Adresse**
- **Autorisierungsinformation zum Sperren des Zertifikats**
- **Verwendungszweck des Zertifikats**
- **Namenskomponenten im Zertifikat**
- **Nachweis der Zugehörigkeit zu einer (zum Leistungsempfang berechtigten) Organisation**

3.2.4 Nicht überprüfte Informationen

Die Regelung ist der entsprechenden CP zu entnehmen.

3.2.5 Überprüfung von Unterschriftsvollmachten

Die Akkreditierung einer handlungsberechtigten Person durch die beantragende Organisation muss in schriftlicher Form erfolgen, es können auch Dokumente verwendet werden, die über eine gültige elektronische Signatur verfügen, sofern dies mit der beantragenden Organisation vereinbart worden ist. Folgende Informationen werden benötigt:

- **Name der handlungsberechtigten Person**
- **E-Mail Adresse**
- **Angaben zum Ausweispapier**

Das Dokument muss von einer Person der beantragenden Organisation gezeichnet werden, die über die entsprechende Unterschriftsvollmacht (siehe Abschnitt 3.2.2) verfügt.

3.2.6 Cross-Zertifizierung

Die Kriterien zur Cross-Zertifizierung sind in der zugehörigen CP beschrieben.

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

3.3.1 Routinemäßige Zertifikaterneuerung

Diese Regelung ist im zugehörigen CP festgelegt.

3.3.2 Zertifikaterneuerung nach einem Widerruf

Diese Regelung ist in der zugehörigen CP festgelegt.

3.4 Identifizierung und Authentifizierung beim einem Widerruf

Für einen Widerruf ist immer die Registrierungsstelle zuständig, bei der das Zertifikat beantragt wurde. Ein Widerruf kann auf folgende Arten erfolgen:

- **Übergabe eines unterzeichneten Sperrantrags mit Angabe der Autorisierungsinformation bzw. Identitätsprüfung nach Abschnitt 3.2.**
- **Übersendung eines unterzeichneten Sperrantrags per Post mit Angabe der Autorisierungsinformation**
- **Übersendung einer digital signierten formlosen E-Mail**
- **Übersendung einer nicht digital signierten formlosen E-Mail mit Angabe der Autorisierungsinformation**
- **Telefonischer Anruf mit Angabe der Autorisierungsinformation**

Kontaktangaben:

E-Mail: **revoke@pca.dfn.de**

Telefon: **+49 40 808077-555**

4 Ablauforganisation

4.1 Zertifikatantrag

4.1.1 Wer kann ein Zertifikat beantragen

Diese Regelung ist in der zugehörigen CP festgelegt.

4.1.2 Registrierungsprozess

Bei der Registrierung werden die folgenden Arbeitsschritte durchlaufen:

- **Prüfung der Dokumente und der CSRs hinsichtlich Vollständigkeit und Korrektheit**
- **Prüfung der Eindeutigkeit des DN im CSR**
- **Archivierung der Dokumente in einem verschlossenem Schrank**
- **Übermittlung der für die Zertifizierung notwendigen Informationen an die zuständige Zertifizierungsstelle erfolgt entweder**
  - **mittels einer verschlüsselten und signierten E-Mail, oder**
  - **auf dem postalischen Weg.**

4.2 Bearbeitung von Zertifikatanträgen

Diese Regelung ist in der zugehörigen CP festgelegt.

4.2.1 Durchführung der Identifikation und Authentifizierung

Diese Regelung ist in der zugehörigen CP festgelegt.

4.2.2 Annahme oder Abweisung von Zertifikatanträgen

Diese Regelung ist in der zugehörigen CP festgelegt.

4.2.3 Bearbeitungsdauer

Die Bearbeitungsdauer beträgt nach Annahme von Zertifikatanträgen grundsätzlich maximal eine Woche.

4.3 Zertifikatausstellung

4.3.1 Weitere Prüfungen der Zertifizierungsstelle

Die Zertifizierungsstelle überprüft die Berechtigung der Registrierungsstelle, ein Zertifikat für den im DN angegebenen Namensraum zu beantragen.

4.3.2 Benachrichtigung des Antragstellers

Das Zertifikat wird im PEM oder PKCS#7 Format an den Zertifikatnehmer entweder

- **auf einem Datenträger durch einen Mitarbeiter der Zertifizierungsstelle, oder**
- **mittels einer signierten E-Mail übergeben.**

4.4 Zertifikatakzeptanz

4.4.1 Annahme des Zertifikats

Ein Zertifikat wird durch den Zertifikatnehmer akzeptiert, wenn

- **das Zertifikat verwendet wird oder**

- **innerhalb von 14 Tagen kein Widerspruch erfolgt.**

Es gelten die Regelungen nach Abschnitt 3.4.

Fehlerhaft ausgestellte Zertifikate werden von der ausstellenden Zertifizierungsstelle bei Kenntnis der Fehlerhaftigkeit unverzüglich widerrufen.

4.4.2 Veröffentlichung des Zertifikats

Ein von der Zertifizierungsstelle ausgestelltes Zertifikat wird grundsätzlich über den Verzeichnisdienst veröffentlicht.

4.4.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist nicht vorgesehen.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Diese Regelungen sind in der zugehörigen CP festgelegt.

4.6 Zertifikaterneuerung / Re-Zertifizierung

Diese Regelungen sind in der zugehörigen CP festgelegt.

4.7 Zertifikaterneuerung / Re-Key

Diese Regelungen sind in der zugehörigen CP festgelegt.

4.8 Zertifikatmodifizierung

Diese Regelungen sind in der zugehörigen CP festgelegt.

4.9 Widerruf und Suspendierung von Zertifikaten

Der Widerruf von Zertifikaten ist in der jeweiligen CP festgelegt, eine Suspendierung von Zertifikaten wird nicht unterstützt. Für die Listen widerrufender Zertifikate (Certificate Revocation List, CRL) gelten folgende Regelungen (Abschnittsnummerierung nach CP):

- **(4.9.7) Veröffentlichungsfrequenz für CRLs**
  Eine aktuelle CRL wird mindestes einmal pro Monat veröffentlicht.
- **(4.9.8) Maximale Latenzzeit für CRLs**
  Bei einer Veränderung wird eine CRL unverzüglich veröffentlicht.
- **(4.9.9) Verfügbarkeit von Online-Widerrufs/Status-Überprüfungsverfahren**
  Die CRLs stehen unter der in 2.1 angegebenen URL zur Verfügung.

4.10 Dienst zur Statusabfrage von Zertifikaten

Ein Online-Status-Überprüfungsverfahren wird nicht angeboten.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatnehmer

Diese Regelungen sind in der zugehörigen CP festgelegt.

4.12 Schlüsselhinterlegung und -wiederherstellung

Die PCA und die CA-Services bieten diese Dienstleistungen nicht an.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

Die Anforderungen an infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen einer Zertifizierungs- bzw. Registrierungsstelle werden durch die angebotenen Dienstleistungen bestimmt. Das konkrete Sicherheitsniveau hinsichtlich der Grundwerte Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität muss in einem Sicherheitskonzept festgeschrieben werden. Das Sicherheitskonzept wird nicht veröffentlicht, aber im Rahmen der Konformitätsprüfung zur Verfügung gestellt.

Sofern in diesem CPS Anforderungen an einzelne Sicherheitsmaßnahmen nicht spezifiziert werden, sind diese grundsätzlich an die entsprechenden Maßnahmenkataloge des IT-Grundschutzhandbuchs anzulehnen.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

5.1.1 Lage und Konstruktion

Die technischen Systeme der PCA und der CA-Services befinden sich in den Räumen der DFN-CERT Services GmbH.

Die Räume bieten hinsichtlich der infrastrukturellen Sicherheitsmaßnahmen einen ausreichenden Schutz, der dem erforderlichen Sicherheitsniveau angemessen ist.

5.1.2 Zutrittskontrolle

Die Betriebsräume der Zertifizierungsstellen sind durch geeignete technische und infrastrukturelle Maßnahmen gesichert. Ein Zutritt zu den Betriebsräumen der Zertifizierungsstelle wird nur Mitarbeitern gestattet, die vom Sicherheitsbeauftragen der PCA autorisiert worden sind. Der Zutritt durch betriebsfremde Personen wird durch eine Besucherregelung festgelegt.

5.1.3 Stromversorgung und Klimatisierung

Die Installation zur Stromversorgung entspricht den erforderlichen Normen, eine Klimatisierung der Räume für die technische Infrastruktur ist vorhanden.

5.1.4 Abwehr von Wasserschäden

Die Räume für die technische Infrastruktur verfügen über einen angemessenen Schutz vor Wasserschäden.

5.1.5 Feuer

Die bestehenden Brandschutzvorschriften werden eingehalten, Handfeuerlöscher sind in ausreichender Anzahl vorhanden.

5.1.6 Datenträger

Es werden folgende Datenträger verwendet:

- **Papier**
- **CD-ROMs**
- **USB-Speichermodule**
- **Magnetbänder**
- **Hardwaretoken**

Datenträger werden in verschlossenen Schränken aufbewahrt. Datenträger mit sensiblen Daten werden in einem Tresor aufbewahrt.

5.1.7 Abfallentsorgung

Informationen auf elektronischen Datenträgern werden sachgemäß vernichtet und anschließend durch einen Dienstleister sachgerecht entsorgt. Papierdatenträger werden mittels vorhandenen Aktenvernichtern zerstört und durch einen Dienstleister sachgerecht entsorgt.

5.1.8 Externes Backup

Findet nicht statt.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitsrelevante Rollen

Um einen ordnungsgemäßen und revisionssicheren Betrieb einer Zertifizierungsstelle zu gewährleisten, ist u.a. eine entsprechende Aufgabenverteilung und Funktionstrennung vorzunehmen.

In der folgenden Tabelle sind in vier Gruppen die sicherheitsrelevanten Rollen definiert, die im Rahmen des Zertifizierungsprozesses erforderlich sind. Jeder Rolle sind dabei bestimmte Tätigkeiten zugeordnet. Die vollständige oder teilweise Kenntnis von PINs und Passwörtern und die Erlaubnis zum Zugriff auf bestimmte Teile der Betriebsinfrastruktur (z.B. Sicherheitsbereiche, Tresore, abgesicherte Betriebsräume) werden anhand der Rollen vorgenommen.

Ein Mitarbeiter kann auch in mehr als einer Rolle auftreten. Dabei ist jedoch zu beachten, dass es Rollenunverträglichkeiten (Abschnitt 5.2.4) gibt. Ebenso ist es möglich, dass Funktionen einer Rolle auf mehrere Mitarbeiter mit dieser Rolle verteilt werden.

Rolle	Funktion	Kürzel
Registrierungsdienst	Schnittstelle zum Zertifikatnehmer. Annahme von Zertifikatanträgen, Prüfung der notwendigen Unterlagen und Annahme von Sperranträgen.	
Teilnehmerservice	Entgegennahme von Zertifikatanträgen und Sperranträgen Identifizierung, Authentifizierung und Prüfung der Autorisierung der Zertifikatnehmer Verifikation der Dokumente Belehrung der Zertifikatnehmer	TS
Registrator	Prüfung des Zertifikatantrags hinsichtlich Vollständigkeit und Korrektheit Archivierung von Dokumenten falls erforderlich Freigabe, Übermittlung von Zertifikatanträgen und Sperr-/Widerrufsanträgen an die zuständige Zertifizierungsstelle	RG

Rolle	Funktion	Kürzel
Zertifizierung	Ausstellen von Zertifikaten und Widerrufslisten, Erzeugung und Verwahrung der CA-Schlüssel.	
CA-Mitarbeiter	Verantwortlich für die Anwendung und Lagerung von elektronischen Datenträgern, auf denen die privaten Schlüssel der Zertifizierungsstelle gespeichert sind. Kenntnis einer Hälfte der PINs (Passwörter) zu den privaten Schlüsseln der Zertifizierungsstelle	CAO1
PIN-Geber	Kenntnis der zweiten Hälfte der PINs (Passwörter) zur Anwendung der privaten Schlüssel der Zertifizierungsstelle.	CAO2
Systembetreuung	Administration der IT-Systeme und dem täglicher Betrieb (Backups usw.).	
System- und Netzwerkadministrator	Installation, Konfiguration, Administration und Wartung der IT- und Kommunikationssysteme. Vollständige Kontrolle über die eingesetzte Hard- und Software, jedoch keinen Zugriff auf und keine Kenntnis von kryptographischen Schlüsseln und deren Passwörtern für Zertifizierungsprozess, Zertifikat- und Sperrmanagement. Ausschließliche Kenntnis der Boot- und Administrator-Passwörter der Systeme.	SA
Systemoperator	Betreuung der Anwendungen (Datensicherung und -wiederherstellung, Web-Server, Zertifikat- und Sperrmanagement).	SO
Überwachung des Betriebs	Keine Funktion im operativen Betrieb, zuständig für die Durchsetzung der in der CP, dem CPS und des Sicherheitskonzeptes festgelegten Grundsätze.	
Revision	Durchführung der betriebsinternen und externen Audits, Überwachung und Einhaltung der Datenschutzbestimmungen	R
Sicherheitsbeauftragter	Definition und Einhaltung der Sicherheitsbestimmungen Überprüfung der Mitarbeiter Vergabe von Berechtigungen Ansprechpartner für sicherheitsrelevante Fragen	ISO

Tabelle 1: Rollen

5.2.2 Involvierte Mitarbeiter pro Arbeitsschritt

In der folgenden Tabelle werden die sicherheitsrelevanten Tätigkeiten beschrieben und den entsprechenden Rollen zugeordnet. Aus der Tabelle ist ebenso zu entnehmen, für welche Tätigkeiten das Vier-Augen-Prinzip eingehalten werden muss.

Tätigkeit	Rollen	Vier-Augen-Prinzip	Erläuterung
Annahme von Zertifikatsanträgen	TS		
Identifizierung und Authentifizierung von Zertifikatnehmern	TS		
Prüfung der Autorisierung von Zertifikatnehmern	TS		
Verifikation von Dokumenten	TS		
Belehrung der Zertifikatnehmer	TS		
Prüfung des DN	TS		
Generierung von Autorisierungsinformationen	TS		Kann auch durch CAO1 wahrgenommen werden.
Annahme und Prüfung von Sperranträgen	TS		TS nimmt den Sperrauftrag entgegen und prüft Autorisierungsinformation.
Prüfung der Anträge hinsichtlich Vollständigkeit und Korrektheit	RG		
Archivierung von Dokumenten sofern erforderlich	RG		
Freigabe und Übermittlung von Zertifikat- und Sperranträgen an die zuständige Zertifizierungsstelle	RG		
Erzeugung von Schlüsselpaaren für selbst betriebene CAs, RAs und Datenverarbeitungssysteme	CAO1, CAO2	x	
Starten von Prozessen zur Erzeugung von Schlüsselpaaren für Zertifikatsnehmer und PIN-Briefen.	CAO1, CAO2	x	
Zertifizierung; Starten von Prozessen zum Ausstellen von Zertifikaten und Widerrufslisten	CAO1, CAO2	x	
Übertragen von Zertifikatrequests zum Zertifizierungsrechner	CAO1		
Veröffentlichen von Zertifikaten und Widerrufslisten	CAO1		
Schlüsselhinterlegung von privaten CA-Schlüsseln für selbst betriebene CAs	CAO1, CAO2	x	
Kenntnis von Boot- und Administrator Passwörtern	SA		
Starten und Stoppen von Prozessen (z.B. Web-Server, Datensicherung)	SO		
Datensicherung	SO, CAO1		CAO1 ermöglicht physikalischen Zugang

Tätigkeit	Rollen	Vier-Augen-Prinzip	Erläuterung
Austausch von Soft- und Hardware Komponenten für			
Zertifizierung	SA, CAO1	x	
andere Systeme	SA, CAO1		CAO1 ermöglicht physikalischen Zugang
Wiedereinspielung von Datensicherungen			
Zertifizierung	SA, CAO1	x	
andere Systeme	SA, CAO1		CAO1 ermöglicht physikalischen Zugang
Überprüfung von Protokolldateien	SA, R		Wird regelmäßig durch SA wahrgenommen, im Rahmen eines Audits durch R
Audit	R		
Vergabe von physikalischen Berechtigungen	ISO		
Technische Vergabe von Berechtigungen	SA, ISO	x	ISO überwacht
Fortschreibung des Betriebs- bzw. Sicherheitskonzepts	ISO		

Tabelle 2: Tätigkeiten und Rollen

5.2.3 Identifizierung und Authentifizierung der Rollen

Die Identifizierung und Authentifizierung der Rollen erfolgt auf Grundlage des in den vorangegangenen Abschnitten vorgestellten Rollenmodells. Der technische Zugang zu den einzelnen IT-Systemen wird durch Benutzerkennung und Passwort[2] realisiert. Der physikalische Zugang zu den einzelnen IT-Systemen wird durch Zutrittskontrollmaßnahmen reglementiert. Der Zugang zum Bankschließfach ist neben dem Besitz des zugehörigen Schlüssels mit einer persönlichen Identifizierung und Authentifizierung verbunden.

5.2.4 Trennung von Aufgaben

In der folgenden Tabelle ist aufgeführt, welche Rollen miteinander unverträglich sind. Bei der Aufteilung der Rollen auf Mitarbeiter wird beachtet, dass einer Person keine miteinander unverträglichen Rollen zugewiesen werden.

Rolle	Unverträglich mit
R - Revision	TS, RG CAO1, CAO2, SA, SO
ISO - Sicherheitsbeauftragter	TS, RG, CAO1, CA02, SA, SO
TS - Teilnehmerservice	R, ISO, SA, SO
RG - Registrator	R, ISO, SA, SO
SA - Systemadministrator	R, ISO, TS, RG, CAO1

[2] *Eine Regelung zum Passwortgebrauch ist vorzuhalten.*

Rolle	Unverträglich mit
SO - Systemoperator	R, ISO, TS, RG, CAO1
CAO1 - CA Mitarbeiter	R, ISO, CAO2, SA, SO
CAO2 - PIN Geber	R, ISO, CAO1

Tabelle 3: Trennung von Aufgaben

Die PCA wählt für ihren Betrieb die folgende Aufteilung der Rollen auf Personengruppen:

Personen-gruppe	Aufgabengebiet	Rollen
1	Überwachung des Betriebs	R, ISO
2	Registrierungsdienst (Teilnehmerservice)	TS
3	Registrierungsdienst (Registrator) und Zertifizierung	RG, CAO1
4	Systembetreuung und PIN-Geber für Zertifizierung	CAO2, SA, SO

Tabelle 4: Aufteilung der Rollen bei der PCA

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an die Mitarbeiter

Die Mitarbeiter der PCA erfüllen alle notwendigen Anforderungen hinsichtlich Vertrauenswürdigkeit, Integrität, Zuverlässigkeit und Fachkunde. Neben einer allgemeinen Ausbildung auf dem Gebiet Informationstechnik verfügen die Mitarbeiter in ihrer Rolle über angemessene Fachkenntnisse in den Bereichen:

- Sicherheitstechnologie, Kryptographie, elektronische Signaturen, PKI,
- Internationale Standards, technische Normen,
- Nationale und internationale Rechtssprechung,
- Unix/Linux Betriebssysteme, TCP/IP Netzwerke und relationale Datenbanken.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Von allen Mitarbeitern der PCA liegt ein polizeiliches Führungszeugnis vor, dieses ist alle zwei Jahre erneut vorzulegen.

Betriebsfremde Personen dürfen nur in Begleitung von autorisierten Mitarbeitern der PCA die Betriebsräume betreten. Die Sicherheitsüberprüfung dieser Personen obliegt dem Unternehmen, bei denen sie angestellt sind.

5.3.3 Anforderungen an die Schulung

In der PCA werden ausschließlich qualifizierte Mitarbeiter eingesetzt. Darüber hinaus werden regelmäßige Schulungen für alle Mitarbeiter der PCA durch kompetente Personen durchgeführt. Ein Mitarbeiter erhält erst nach Nachweis der notwendigen Fachkunde eine Berechtigung, eine spezifische Rolle auszuführen.

5.3.4 Frequenz von Schulungen

Die Frequenz der Schulungen orientiert sich an den Anforderungen der PCA. Schulungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

5.3.5 Ablauf und Sequenz der Job Rotation

Der Ablauf und die Sequenz der Job Rotation richtet sich nach den Anforderungen der PCA oder eines bestimmten Mitarbeiters. Ein Arbeitsplatztausch ist nicht zwingend erforderlich.

5.3.6 Sanktionen für unautorisierte Handlungen

Unautorisierte Handlungen, die die Sicherheit der IT-Systeme der PCA gefährden oder gegen Datenschutzbestimmungen verstoßen, werden disziplinarisch geahndet. Bei strafrechtlicher Relevanz werden die zuständigen Behörden informiert.

5.3.7 Anforderungen an die Arbeitsverträge

Für die Arbeitsverträge der Mitarbeiter der PCA gilt das Recht der Bundesrepublik Deutschland. Alle Mitarbeiter sind gemäß den gesetzlichen Datenschutzbestimmungen zur Geheimhaltung verpflichtet.

5.3.8 Dokumente für die Mitarbeiter

Den Mitarbeitern der PCA stehen folgende Dokumente zur Verfügung:

- **Zertifizierungsrichtlinie (CP)**
- **Erklärung zum Zertifizierungsbetrieb (CPS)**
- **Betriebshandbuch**
  - **Dienstleistungen**
  - **Sicherheitskonzept**
  - **Prozessbeschreibungen und Formulare für den regulären Betrieb**
  - **Verfahrensanweisungen für den Notfall**
  - **Dokumentation der IT-Systeme**
  - **Bedienungsanleitung für die eingesetzte Software**

5.4 Sicherheitsüberwachung

5.4.1 Überwachte Ereignisse

Zur Abwehr von Angriffen und zur Kontrolle der ordnungsgemäßen Funktion der PCA werden die nachfolgenden Maßnahmen ergriffen. Folgende Klassen von Ereignissen werden in Form von Log-Dateien oder Papierprotokollen erfasst:

- **Betrieb der IT-Komponenten, u.a.**
  - **Bootvorgänge der Hardware**
  - **Fehlgeschlagene Login-Versuche**
  - **Vergabe und Entzug von Berechtigungen**
  - **Installation und Konfiguration der Software**
- **Alle Transaktionen der Zertifizierungsstelle, u.a.**
  - **Zertifikatanträge**
  - **Zertifikatauslieferung**
  - **Zertifikatveröffentlichung**
  - **Zertifikatrevokation**
  - **Schlüsselerstellung**
  - **Zertifikaterstellung**
- **Änderungen der Richtlinien und des Betriebshandbuchs, u.a.**
  - **Rollendefinitionen**
  - **Prozessbeschreibungen**
  - **Wechsel der Verantwortlichkeiten**

5.4.2 Frequenz der Protokollanalyse

Eine Überprüfung der Protokolldaten findet regelmäßig statt, jedoch mindestens einmal pro Monat. Bei Verdacht auf außergewöhnliche Ereignisse werden Sonderprüfungen vorgenommen.

5.4.3 Aufbewahrungszeitraum für Protokolldaten

Sicherheitsrelevante Protokolldaten werden entsprechend den gesetzlichen Regelungen aufbewahrt. Die Aufbewahrungsdauer von Protokolldaten bezüglich des Schlüssel- und Zertifikatmanagements entspricht der Gültigkeitsdauer des Zertifikats der Zertifizierungsstelle, zuzüglich eines Jahres.

5.4.4 Schutz der Protokolldaten

Elektronische Log-Dateien werden mit Mitteln des Betriebssystems gegen Zugriff, Löschung und Manipulation geschützt und sind nur den System- und Netzwerkadministratoren zugänglich.

5.4.5 Backup der Protokolldaten

Die Protokolldaten werden zusammen mit anderen relevanten Daten der PCA einem regelmäßigen Backup unterzogen. Protokolle auf Papier werden in verschließbaren Schränken verwahrt.

5.4.6 Überwachungssystems

Es wird ein internes Überwachungssystemsystem verwendet.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Bei schwerwiegenden Ereignissen wird unverzüglich der Sicherheitsbeauftragte informiert. In Zusammenarbeit mit den Systemadministratoren werden notwendige Aktionen festgelegt, um auf die Ereignisse adäquat reagieren zu können, ggf. wird die Geschäftsleitung informiert.

5.4.8 Schwachstellenuntersuchung

Eine Schwachstellenuntersuchung findet durch die PCA selbst bzw. durch den Hersteller der verwendeten Software statt.

5.5 Archivierung

5.5.1 Archivierte Daten

Archiviert werden Daten, die für den Zertifizierungsprozess relevant sind:

- **Zertifikatanträge, diese enthalten persönliche Daten des Zertifikatnehmers**
- **Alle von der Zertifizierungsstelle ausgestellten Zertifikate**
- **Widerrufsanträge**
- **Widerrufslisten (CRLs)**

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Es gelten die Regelungen, die in Abschnitt 5.4.3. beschrieben werden.

5.5.3 Schutz der Archive

Es wird durch geeignete Maßnahmen sichergestellt, dass die Daten nicht verändert oder gelöscht werden können. Sind in den Archiven personenbezogene Daten enthalten, wird

darüber hinaus sichergestellt, dass die Daten nicht unbefugt gelesen oder kopiert werden können.

5.5.4 Datensicherungskonzept

Die in den Abschnitten 5.4.1 und 5.5.1 aufgeführten Daten werden auf Grundlage eines Datensicherungskonzepts regelmäßig mit einer Offline-Sicherung auf Band oder CD-ROM unterzogen. Eckwerte des Datensicherungskonzepts:

- inkrementelles Backup an jedem Werktag
- wöchentliches vollständiges Backup
- monatliches Archivbackup

Die Backupmedien werden geeignet außerhalb des Serverraums aufbewahrt. Das Archivbackup wird in einem Bankschließfach verwahrt.

5.5.5 Anforderungen für Zeitstempel

Keine Bestimmungen.

5.5.6 Archivierungssystem

Es wird ein internes Archivierungssystem verwendet.

5.5.7 Prozeduren zum Abrufen und Überprüfen von archivierten Daten

Der Sicherheitsbeauftragte kann den Abruf und die Prüfung der archivierten Daten autorisieren.

5.6 Schlüsselwechsel

Die Gültigkeitsdauer von Schlüsseln ist in Abschnitt 6.3.2 festgelegt. Die Regelungen für einen Schlüsselwechsel bei Zertifikatnehmern in der zugehörigen CP festgelegt. Falls ein Schlüssel der Zertifizierungsstelle kompromittiert wurde, gelten die in Abschnitt 5.7.3. aufgeführten Regelungen.

5.7 Kompromittierung und Wiederherstellung

5.7.1 Prozeduren bei Sicherheitsvorfällen und Kompromittierung

Die Prozeduren zur Behandlung von Sicherheitsvorfällen und bei der Kompromittierung von privaten Schlüsseln der Zertifizierungsstelle sind in einer Verfahrensanweisung für den Notfall dokumentiert. Diese Anweisung wird an alle Mitarbeiter ausgehändigt. Die Grundzüge der Prozeduren sind in den folgenden Abschnitten aufgeführt.

5.7.2 Prozeduren bei IT-Systemen

Werden innerhalb der Zertifizierungsstelle fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der Zertifizierungsstelle haben, wird der Betrieb des entsprechenden IT-Systems unverzüglich eingestellt.

Das IT-System wird auf einer Ersatzhardware unter Wiederherstellung der Software und der Daten aus der Datensicherung neu aufgesetzt, überprüft und in einem sicheren Zustand in Betrieb genommen. Anschließend wird das fehlerhafte oder modifizierte IT-System analysiert. Bei Verdacht einer vorsätzlichen Handlung werden gegebenenfalls rechtliche Schritte eingeleitet. Darüber hinaus erfolgen eine Bewertung der Sicherheit und eine Revision zur Aufdeckung von Schwachstellen. Gegebenenfalls werden zusätzliche Abwehrmaßnahmen zur Vermeidung ähnlicher Vorfälle ergriffen. Die Mitarbeiter der Zertifizierungsstelle arbeiten in diesen Fällen mit den Experten des DFN-CERTs zusammen. Falls sich in einem Zertifikat

fehlerhafte Angaben befinden, wird der Zertifikatnehmer unverzüglich informiert und das Zertifikat widerrufen.

5.7.3 Kompromittierung von privaten Schlüsseln der Zertifizierungsstelle

Wurde der private Schlüssel der Zertifizierungsstelle kompromittiert, oder besteht ein begründeter Verdacht auf eine Kompromittierung, so wird umgehend der Sicherheitsbeauftragte der Zertifizierungsstelle informiert. Dieser überprüft eine festgestellte Kompromittierung oder einen Verdacht und ordnet gegebenenfalls den Widerruf betroffener Zertifikate an. In diesem Fall werden folgende Maßnahmen ergriffen:

- **Unverzügliche Information aller direkt betroffenen Zertifikatnehmer.**
- **Widerruf des Zertifikats der Zertifizierungsstelle und aller Zertifikate, die mit dem Zertifikat zertifiziert wurden. Gegebenenfalls Abschaltung der Verzeichnisdienste und der Statusabfragen, um inkorrekte oder ungültige Aussagen durch die Dienste zu verhindern.**
- **Erzeugung eines neuen Schlüsselpaares und eines Zertifikats für die Zertifizierungsstelle.**
- **Veröffentlichung des Zertifikats der Zertifizierungsstelle**
- **Ausstellung neuer Zertifikate für die Zertifikatnehmer nach Vorgabe durch den Sicherheitsbeauftragten**

5.7.4 Betrieb nach einer Katastrophe

Eine Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe bei Verlust ist Bestandteil der Notfallplanung und kann innerhalb kurzer Zeit erfolgen, sofern die Sicherheit der Zertifizierungsdienstleistung gegeben ist. Die Bewertung der Sicherheitslage obliegt dem Sicherheitsbeauftragten.

5.8 Einstellung des Betriebs

Falls es zur Einstellung des Zertifizierungsbetriebs kommen sollte, werden folgende Maßnahmen ergriffen:

- **Information aller Zertifikatnehmer, Registrierungsstellen und betroffenen Organisationen mindestens drei Monate vor Einstellung der Tätigkeit.**
- **Rechtzeitiger Widerruf aller Zertifikate.**
- **Sichere Zerstörung der privaten Schlüssel der Zertifizierungsstelle.**

Der DFN-Verein stellt den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen Widerrufsliste für den zugesicherten Aufbewahrungszeitraum sicher.

6 Technische Sicherheitsmaßnahmen

Die Anforderungen an technische Sicherheitsmaßnahmen einer Zertifizierungs- bzw. Registrierungsstelle werden durch die angebotenen Dienstleistungen bestimmt. Das konkrete Sicherheitsniveau hinsichtlich der Grundwerte Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität muss in einem Sicherheitskonzept festgeschrieben werden. Das Sicherheitskonzept wird nicht veröffentlicht, aber im Rahmen der Konformitätsprüfung zur Verfügung gestellt.

Sofern in diesem CPS Anforderungen an einzelne Sicherheitsmaßnahmen nicht spezifiziert werden, sind diese grundsätzlich an die entsprechenden Maßnahmenkataloge des IT-Grundschutzhandbuchs anzulehnen.

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Die Schüsselpaare der PCA, der CA-Services sowie für die eingesetzten Datenverarbeitungssysteme werden auf einem dezidierten IT-System erzeugt, welches über keinen Netzwerkanschluss verfügt. Die Schlüssel werden ausschließlich auf einem externen Datenträger gespeichert und durch eine PIN gesichert.

6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatnehmer

Für Zertifikatnehmer werden keine kryptographischen Schlüsselpaare erzeugt.

6.1.3 Auslieferung des öffentlichen Schlüssels an den Zertifikatausssteller

Der CSR des Zertifikatnehmers wird durch die Registrierungsstelle der Zertifizierungsstelle im PKCS#10 Format mittels signierter E-Mail übermittelt. Sollte dies nicht möglich sein, z.B. bei im Aufbau befindlichen Registrierungs- und Zertifizierungsstellen, werden die öffentlichen Schlüssel der zuständigen Registrierungs- bzw. Zertifizierungsstelle durch eine handlungsberechtigte Person auf einem Datenträger übergeben.

6.1.4 Auslieferung des öffentlichen CA-Schlüssels

Alle Teilnehmer der DFN-PKI können den öffentlichen Schlüssel der PCA und der CA-Services im PEM-, PKCS#7-Format oder in binärer Form (DER) über den Verzeichnisdienst (siehe 2.1) abrufen.

6.1.5 Schlüssellängen

Die eingesetzten kryptographischen Algorithmen und deren Schlüssellängen orientieren sich an den Veröffentlichungen der Regulierungsstelle für Telekommunikation und Post [REGTP]:

- **Als Signaturverfahren wird der RSA-Algorithmus (mit SHA1 Prüfsummen) eingesetzt,**
- **die Schlüssellänge beträgt bei Zertifizierungsstellen min. 2048 Bit,**
- **bei allen anderen Schlüsseln müssen min. 1024 Bit verwendet werden. Für die Gewährleistung eines langfristigen Sicherheitsniveaus wird aber die Verwendung von min. 2048 Bit empfohlen.**

6.1.6 Parameter der öffentlichen Schlüssel und Qualitätssicherung

Die Parameter werden von der Zertifizierungsstelle erzeugt. Diese werden bei ihrer Erzeugung sorgfältig ausgewählt.

6.1.7 Verwendungszweck der Schlüssel und Beschränkungen

Verwendungszweck der Schlüssel und Beschränkungen werden im entsprechenden X.509 v3 Feld (*keyUsage)* festgelegt (siehe 7.1.2).

6.2 Schutz des privaten Schlüssels

Erfolgt die Anwendung des privaten Schlüssels der Zertifizierungsstelle auf einem vernetzen IT-System, so muss der private Schlüssel nicht auslesbar auf einem Hardware-Sicherheitsmodul (Hardware Security Module, HSM) gespeichert werden. Diese Anforderung entfällt, wenn die Anwendung auf einem dezidierten und nicht vernetzten IT-System erfolgt. Es ist jedoch sicherzustellen, dass nach Anwendung des privaten Schlüssels keine Schlüssel auf dem IT-System verbleiben.

6.2.1 Standard des kryptographischen Moduls

Werden HSM-Module im Rahmen der Zertifizierung eingesetzt, muss das Modul einem der folgend genannten oder einem äquivalenten Standard genügen:

- **FIPS 140-1 Level 3**
- **CC EAL4 oder ITSEC E3 der Stärke „hoch“**

6.2.2 Teilung des privaten Schlüssels

Eine Teilung der privaten Schlüssel der PCA und der CA-Services ist nicht vorgesehen.

6.2.3 Hinterlegung privater Schlüssel

Eine Hinterlegung privater Schlüssel von Zertifikatnehmern findet nicht statt.

6.2.4 Backup der privaten Schlüssel

Ein Backup der privaten Schlüssel von Zertifikatnehmern findet nicht statt. Von den Schüsselpaaren der PCA und der CA-Services werden Kopien angefertigt und auf Datenträgern in einem Bankschließfach aufbewahrt. Die privaten Schlüssel sind durch eine PIN gesichert. Schriftliche Kopien der beiden PIN-Hälften werden in einem versiegelten Umschlag in einem zweiten Bankschließfach oder bei einem Notar hinterlegt. Der Zugang zu diesen Schließfächern ist streng reglementiert.

6.2.5 Archivierung der privaten Schlüssel

Eine Archivierung der privaten Schlüssel von Zertifikatnehmern findet nicht statt.

6.2.6 Installation privater Schlüssel in einem kryptographischen Modul

Entfällt.

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Entfällt.

6.2.8 Aktivierung der privaten Schlüssel

Die Aktivierung eines privaten Schlüssels erfolgt durch Eingabe eines Passworts bzw. einer PIN.

Bei privaten Schlüsseln der Zertifizierungsstelle wird die PIN in zwei Hälften unterteilt. Diese sind anteilig nur den Rollen „CAO1“ und „CAO2“ bekannt. Eine Aktivierung ist nur nach dem Vier-Augen-Prinzip möglich.

6.2.9 Deaktivierung der privaten Schlüssel

Die Deaktivierung der privaten Schlüssel erfolgt automatisch. Nach Beendigung des Zertifizierungsprozesses (dies kann auch ein Batch-Prozess sein) wird die weitere Verwendung des privaten Schlüssels durch technische Maßnahmen unterbunden.

6.2.10 Vernichtung der privaten Schlüssel

Bei der Vernichtung der privaten Schlüssel der PCA und der von ihr betreiben Zertifizierungsstellen wird nach dem Vier-Augen-Prinzip verfahren. Verantwortlich für die Vernichtung sind die Rollen „ISO“ und „CAO1“.

6.2.11 Güte des Kryptographischen Moduls

Siehe 6.2.1.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel werden sowohl im Verzeichnisdienst als auch auf Medien für die Datensicherung archiviert.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Die von der PCA und den CA-Services ausgestellten Zertifikate haben folgende Gültigkeitszeiträume:

- **Wurzel-Zertifikat der PCA maximal acht (8) Jahre und zwei (2) Monate**
- **Zertifikate für CAs maximal vier (4) Jahre**
- **Alle anderen Zertifikate maximal zwei (2) Jahre**

Die Nutzungsdauer von Schlüsselpaaren entspricht grundsätzlich der Gültigkeitsdauer der darauf basierenden Zertifikate. Eine Verwendung von vorhandenen Schlüsselpaaren im Rahmen einer Re-Zertifizierung ist zulässig, wenn die empfohlenen Algorithmen und Schlüssellängen dies erlauben (siehe Abschnitt 6.1.5).

6.4 Aktivierungsdaten

Für Passwörter bzw. PINs zur Aktivierung von privaten Schlüsseln sollten nicht triviale Kombinationen aus alphanumerischen Zeichen und Sonderzeichen gewählt werden. Die Länge sollte mindestens 8 Zeichen lang sein.

Im Rahmen der Zertifizierung werden bei der PCA Aktivierungsdaten verwendet, bei denen die Anzahl der Zeichen mindestens 15 beträgt. In allen anderen Fällen müssen mindestens 8 Zeichen verwendet werden.

6.4.1 Aktivierungsdaten für Erzeugung und Installation

Entfällt.

6.4.2 Schutz der Aktivierungsdaten

Aktivierungsdaten müssen geheim gehalten werden und dürfen nur den Mitarbeitern bekannt sein, die diese nach Abschnitt 5.2.1 für die Durchführung einer spezifischen Funktion benötigen. Eine schriftliche Fixierung ist allenfalls für die Hinterlegung nach Abschnitt 6.2.4 zulässig.

6.4.3 Weitere Aspekte

Entfällt.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

Alle Anwendungen innerhalb der Zertifizierungsstelle werden ausschließlich auf Basis von gehärteten Betriebssystemen betrieben. Darüber hinaus werden folgende Sicherheitsmaßnahmen umgesetzt:

- **Zugriffskontrolle**
- **Benutzerauthentifizierung**

6.5.2 Güte / Qualität der Sicherheitsmaßnahmen

Keine Angaben.

6.6 Lebenszyklus der Sicherheitsmaßnahmen

6.6.1 Softwareentwicklung

Keine Bestimmungen. Der Einsatz von Software (Eigen- oder Fremdentwicklung) erfolgt jedoch erst nach Abnahme und Freigabe.

6.6.2 Sicherheitsmanagement

Das Sicherheitsmanagement umfasst folgende Aspekte:

- **jährliches Audit (Konformitätsprüfung)**
- **Regelmäßige Evaluierung und Weiterentwicklung des Sicherheitskonzepts**
- **Überprüfung der Sicherheit im laufenden Betrieb (siehe auch Abschnitt 5.4)**
- **Regelmäßige Integritätsprüfungen der eingesetzten Anwendungen und Betriebssysteme**
  - **Zentrales Logging aller sicherheitsrelevanten Vorgänge**
  - **Zusammenarbeit mit dem DFN-CERT**
  - **Einspielung von Upgrades und Patches sofern erforderlich**
  - **Einsatz auf einem Produktivsystem erst nach Freigabe auf einem Testsystem**

6.6.3 Sicherheitseinstufung

Eine Sicherheitseinstufung wird nicht vorgenommen.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Das Netzwerk der Zertifizierungsstelle ist in verschiedene Sicherheitszonen unterteilt, die jeweils durch eine Firewall voneinander abgeschottet sind. Darüber hinaus werden zur Abwehr von Angriffen aus dem Internet, wie auch aus dem Intranet, Intrusion Prevention bzw. Detection Systeme eingesetzt. Kritische Sicherheitsvorfälle werden unverzüglich in Zusammenarbeit mit dem DFN-CERT verfolgt und bearbeitet.

Auf allen vernetzten IT-Systemen sind darüber host-basierte Firewalls installiert, die nur den in einer definierten Kommunikationsmatrix erlaubten Netzwerkverkehr zulassen.

6.8 Zeitstempel

Die ausgegebenen Zertifikate verfügen über keinen Zeitstempel.

7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

In diesem Abschnitt werden die Profile, Eigenschaften und Erweiterungen, die in Zertifikaten, Widerrufslisten und Online-Statusabfragen verwendet werden, beschrieben. Zugrunde gelegt werden im Syntax und Semantik nach X.509 [X.509], der IETF Arbeitsgruppe PKIX „Public Key Infrastructure (X.509)“ [PKIX] und verbreitete Industriestandards wie sie etwa von Netscape [NETS] mit den Netscape Certificate Extensions und RSA mit [PKCS] festgelegt wurden.

7.1 Zertifikatprofil

7.1.1 Versionsnummer

Zertifikate werden entsprechend der internationalen Norm X.509 in der Version 3 ausgestellt.

7.1.2 Zertifikaterweiterungen

Die folgenden Zertifikaterweiterungen werden in den ausgestellten Zertifikaten verwendet:

	Wurzel	SubCA	Nat. Person / Rolle	DV-System-Server	DV-System-Client	Critical	Optional	Pflicht
Identifikator des Zertifikatnehmerschlüssels (Subject Key Identifier): KeyID (Hash) des öffentlichen Schlüssels des Zertifikatnehmer	x	x	x	x	x			x
Identifikator des Zertifikatgeberschlüssels (Authority Key Identifier): KeyID (Hash) des öffentlichen Schlüssels des Zertifikatgebers.	x	x	x	x	x			x
URLs für Widerrufslisten (CRL Distribution Points, CDPs): Mehrere CDPs in Form von HTTP URIs	x	x	x	x	x			x
Basis Beschränkungen (Basic Constraints): CA=TRUE	x	x				x		x
Basis Beschränkungen (Basic Constraints): CA=FALSE			x	x	x	x		x
Schlüsselnutzungszweck (Key Usage): Certificate Sign	x	x				x		x
Schlüsselnutzungszweck (Key Usage): CRL Sign	x	x				x		x
Schlüsselnutzungszweck (Key Usage): Digital Signature			x	x	x	x		x
Schlüsselnutzungszweck (Key Usage): Key Encipherment			x	x	x	x		x
Schlüsselnutzungszweck (Key Usage): Data Encipherment			x		x	x		x
Erweiterter Schlüsselnutzungszweck (Extended Key Usage) clientAuth (nach PKIX)			x		x		x	
Erweiterter Schlüsselnutzungszweck (Extended Key Usage) codeSigning (nach PKIX)			x		x		x	
Erweiterter Schlüsselnutzungszweck (Extended Key			x		x		x	

	Wurzel	SubCA	Nat. Person / Rolle	DV-System-Server	DV-System-Client	Critical	Optional	Pflicht
Usage) emailProtection (nach PKIX)								
Erweiterter Schlüsselnutzungszweck (Extended Key Usage) serverAuth (nach PKIX)				x			x	
Erweiterter Schlüsselnutzungszweck (Extended Key Usage) ipsecEndSystem (nach PKIX)				x	x		x	
Erweiterter Schlüsselnutzungszweck (Extended Key Usage) ipsecTunnel (nach PKIX)				x	x		x	
Erweiterter Schlüsselnutzungszweck (Extended Key Usage) ipsecUser (nach PKIX)			x				x	
Erweiterter Schlüsselnutzungszweck (Extended Key Usage) smartCardLogin (nach Microsoft)			x				x	
Netscape Zertifikat Typ (Netscape Certificate Type): SSL CA	x							x
Netscape Zertifikat Typ (Netscape Certificate Type): S/MIME CA	x							x
Netscape Zertifikat Typ (Netscape Certificate Type): Object Signing CA	x							x
Netscape Zertifikat Typ (Netscape Certificate Type): SSL CA		x					x	
Netscape Zertifikat Typ (Netscape Certificate Type): S/MIME CA		x					x	
Netscape Zertifikat Typ (Netscape Certificate Type): Object Signing CA		x					x	
Information zum Auffinden des Zertifikates der ausstellenden Zertifizierungsstelle (authorityInfo-Access, caIssuers): URI		x	x	x	x		x	
Optional alternativer Name des Zertifikatnehmers (subjectAltName): ein oder mehrere DNS Namen				x			x	
Optional alternativer Name des Zertifikatnehmers (subjectAltName): ein oder mehrere E-Mail Adressen			x		x		x	
Optional alternativer Name des Zertifikatnehmers (subjectAltName): ein oder mehrere IP Nummern				x			x	
Optional alternativer Name des Zertifikatgebers (issuerAltName): ein oder mehrere E-Mail Adressen		x	x	x	x		x	
Objekt Identifikator für die Zertifizierungsrichtlinie (CP): OID der CP (siehe Abschnitt 1.2 der CP) und URIs von der CP und des CPS			x	x	x			x

Tabelle 5: Zertifikaterweiterungen

Andere Zertifikaterweiterungen:

Zusätzliche Zertifikaterweiterungen und erweiterte Schlüsselnutzungszwecke können eingesetzt werden, wenn diese in dem jeweiligen CPS aufgeführt sind.

Schlüsselhinterlegung:

Das „nonRepudiation“ Flag darf in einem nur Zertifikat gesetzt werden, wenn keine Wiederherstellung des privaten Schlüssels durch die Zertifizierungsstelle oder einen Dritten möglich ist.

Seriennummern:

Seriennummern für ausgestellte Zertifikate werden von einer ausstellenden Zertifizierungsstelle nicht zweimal vergeben und sind somit eindeutig in Bezug auf die ausstellende Zertifizierungsstelle (identifiziert durch den DN).

7.1.3 Objekt Identifikatoren von Algorithmen

Objekt Identifikatoren für Algorithmen werden nach PKIX verwendet.

7.1.4 Namensformen

Namensformen für Zertifikate sind gemäß der Spezifikationsserie X.500 zu wählen. Namen können sowohl nach klassischem X.509 Modell mit C, ST, L, O, OU und CN Einträgen als auch nach dem neueren Domain-Komponenten-Modell (Domain Components, DC) mit den aus dem DNS bekannten aufgeschlüsselten DC Einträgen bestehen.

7.1.5 Namensbeschränkungen

Siehe 3.1.

7.1.6 Objekt Identifikator der CP

Der Objekt Identifikator der zugehörigen CP wird nach Abschnitt 1.2 (CP) gesetzt. Weiter wird eine URL zum leichteren Auffinden von CP und CPS bereitgestellt.

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkung

Keine.

7.1.8 Syntax und Bedeutung von Richtlinienkennungen

Siehe 1.2.

7.1.9 Abarbeitung von kritischen Erweiterungen der CP

Keine.

7.2 CRL Profil

7.2.1 Versionsnummer

Widerrufslisten werden gemäß der internationalen Norm X.509 in der Version 1 erstellt.

7.2.2 Erweiterungen von CRL und CRL Einträgen

Keine.

7.3 OCSP Profil

Von der PCA wird kein OCSP angeboten.

8 Konformitätsprüfung

Die Regelungen sind der zugehörigen CP zu entnehmen.

9 Rahmenvorschriften

Die Regelungen sind der zugehörigen CP zu entnehmen.

10 Glossar

	Englisch	Deutsch
ASN.1	Abstract Syntax Notation One	Abstrakte Syntaxnotation Nummer 1, Datenbeschreibungssprache der Anwendungsschicht des OSI-Modells
CA	Certification Authority	Zertifizierungsstelle
Certificate	Certificate	Zertifikat – Zuordnung eines Kryptographischen Schlüssels (siehe Private Key) zu einer Identität, welches von einer CA signiert wurde
CN	Common Name	Name (Bestandteil des Distinguished Names)
CRL	Certificate Revocation List	Liste widerrufender Zertifikate
CP	Certificate Policy	Zertifizierungsrichtlinie
CPS	Certification Practice Statement	Erklärung zum Zertifizierungsbetrieb - praktische (technisch und organisatorisch) Umsetzung der Zertifizierungsrichtlinie
CSR	Certificate Signing Request	Zertifizierungsanfrage
DC	Domain Component	Standard für Namen im DN oder Knoten im LDAP Verzeichnisdienst
DER	Distinguished Encoding Rules	Codierungsregeln für ASN.1-Daten
DFN	abbr.: The National Research and Education Network in Germany	Deutsches Forschungsnetz
DN	Distinguished Name	Hervorragender oder eindeutiger Name (X.500 - ein DN bildet sich aus den Werten aller Objekte von der Wurzel bis zum entsprechenden Eintrag.)
DNS	Domain Name System	Standard für Internet Namen
DS	Digital Signature	Digitale (elektronische) Signatur
EB-CA	European Bridge-CA	Initiative zur Verknüpfung von PKIs zwischen Wirtschaft und öffentlicher Verwaltung
EXT	External	Kennzeichen für externe Zertifikatnehmer im CN
GRP	Group	Kennzeichen für Personen- bzw. Funktionsgruppen im CN
HSM	Hardware Security Module	Bauteil, das sicherheitsrelevante Informationen wie Daten und kryptographische Schlüssel sicher speichert und verarbeitet
I	Issuer	Beschreibung des Zertifikatausstellers
IETF	Internet Engineering Task Force	Projektgruppe der Internet Society zum technischen Aufbau des Internets
LDAP	Lightweight Directory Access Protocol	Protokoll zur Nutzung von Verzeichnisdiensten

	Englisch	Deutsch
O	Organization	Organisation (Bestandteil des DN)
OCSP	Online Certification Status Protocol	Protokoll zur Prüfung des aktuellen Status eines Zertifikats
OID	Object Identifier	Objekt Identifikator – eindeutige Referenz auf ein Objekt in einem Namensraum
OSI	Open Systems Interconnection Reference Model	Standardisiertes Referenzmodell der ISO für Kommunikationsprotokolle
OU	Organizational Unit	Organisationseinheit (Bestandteil des DN)
PCA	Policy Certification Authority	Oberste Zertifizierungsstelle der DFN-PKI - gibt die Regeln (Policy) vor, die alle nachgeordneten CAs einhalten müssen
PEM	Privacy Enhanced Mail	Technischer Standard (RFC), Sicherheitsdienste für E-Mail
PIN	Personal Identification Number	Persönliches numerisches Passwort
PKCS	Public Key Cryptography Standard	Spezifikationen asymmetrischer Verschlüsselungsverfahren der Firma RSA Security.
PKCS#7	Cryptographic Message Syntax Standard	Syntax für kryptographische Nachrichten
PKCS#10	Certification Request Syntax Standard	Syntax eines Zertifikatantrags
PKI	Public Key Infrastruktur	Bezeichnung für die notwendigen technischen Einrichtungen sowie der dazugehörenden Prozesse und Konzepte bei der asymmetrischen Verschlüsselung
PKI-1 Verwaltung	PKI within public administration	PKI im Bereich öffentlicher Verwaltung in Deutschland
PN	Pseudonym	Kennzeichen für Pseudonyme im CN
Private Key	Private Key	Privater Schlüssel - Schlüssel eines kryptographischen Schlüsselpaares, welcher nur dem Eigentümer zugänglich ist. Ein privater Schlüssel kann z.B. zur Erzeugung von elektronischen Signaturen verwendet werden.
PSE	Personal Secure Environment	Umgebung zur Speicherung persönlicher u. sicherheitsrelevanter Daten (z.B. Chipkarte)
Public Key	Public Key	Öffentlicher Schlüssel - Schlüssel eines kryptographischen Schlüsselpaares, welcher öffentlich bekannt gemacht wird. Ein öffentlicher Schlüssel kann z.B. zur Überprüfung von elektronischen Signaturen verwendet werden.
PKIX	Public Key Infrastructure (X.509)	Eine Serie von Spezifikationen der IETF im Umfeld von digitalen Zertifikaten nach X.509 Spezifikation
RA	Registration Authority	Registrierungsstelle

	Englisch	Deutsch
RFC	**Request for Comments**	**Traditionelle Bezeichnung von technischen Standards im Internet**
S	**Subject**	**Subjekt (Identität des Zertifikatnehmers)**
SigG	**German Signature Act**	**Deutsches Signaturgesetz**
SSL	**Secure Socket Layer**	**Ein Protokoll für die sichere Kommunikation im Internet**
URL	**Uniform Resource Locator**	**Eindeutige Bezeichnung einer Ressource im Internet**
V-PKI	**See PKI-1 Verwaltung**	**Siehe PKI-1 Verwaltung**
VPN	**Virtual Private Network**	**Verwendung von Verschlüsselungsverfahren auf unteren Protokollebenen, um über ein unsicheres Netz sicher kommunizieren zu können**
X.509v3	**International standard for the definition of electronic certificates (Version 3)**	**Internationaler Standard für die Definition von elektronischen Zertifikaten (Version 3)**

11 Referenzen

[BDSG]	**Datenschutzgesetz, Bundesgesetzblatt I 2003 S.66.**
[CP-Classic]	**Zertifizierungsrichtlinie (CP) – Sicherheitsniveau Classic, Version 1.1, DFN-Verein, 2005**
[CPS-Classic]	**Erklärung zum Zertifizierungsbetrieb (CPS) – Sicherheitsniveau Classic, Version 1.1, DFN-Verein, 2005**
[EU-RL]	**Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 1999/93/EG, EU, 1999**
[NETS]	**Netscape Certificate Extensions, Communicator 4.0 Version, http://wp.netscape.com/eng/security/comm4-cert-exts.html**
[REGTP]	**Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung – Geeignete Algorithmen, Regulierungsbehörde für Telekommunikation und Post, Bundesanzeiger Nr. 30, S.2537-2538, 13.02.2004**
[PKCS]	**RSA Security Inc., RSA Laboratories „Public Key Cryptography Standards“, http://www.rsasecurity.com/rsalabs**
[PKIX]	**RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)**
[RFC2527]	**Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 1999**
[RFC3647]	**Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003**
[SigG]	**Gesetz über Rahmenbedingungen für elektronische Signaturen, Bundesgesetzblatt I 2001, S. 876**
[X.509]	**Information technology - Open Systems Interconnection - The Directory: authentication framework, Version 3, ITU, 1997**