Zertifizierungsrichtlinie der

Public Key Infrastruktur

im Deutschen Forschungsnetz

- Basic -

DFN-Verein

CP-Basic V1.1, Februar 2005

Dieses Dokument einschließlich aller Teile ist urheberrechtlich geschützt.

Die unveränderte Weitergabe (Vervielfältigung) ist ausdrücklich erlaubt.

Die Überführung in maschinenlesbare oder andere veränderbare Formen der elektronischen Speicherung, auch auszugsweise, ist ohne Zustimmung des DFN-Vereins unzulässig.

Kontakt: pki@dfn.de

© DFN-Verein 2005

Inhaltsverzeichnis

1 Einleitung 5
1.1 Überblick 5
1.2 Identifikation des Dokuments 6
1.3 Teilnehmer der Zertifizierungsinfrastruktur 6
1.4 Anwendungsbereich 8
1.5 Verwaltung der Richtlinien 8
1.6 Definitionen und Abkürzungen 8
2 Veröffentlichungen und Verzeichnisdienst 10
2.1 Verzeichnisdienst 10
2.2 Veröffentlichung von Informationen 10
2.3 Aktualisierung der Informationen 10
2.4 Zugang zu den Informationsdiensten 10
3 Identifizierung und Authentifizierung 11
3.1 Namen 11
3.2 Identitätsüberprüfung bei Neuantrag 12
3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung 14
3.4 Identifizierung und Authentifizierung bei einem Widerruf 14
4 Ablauforganisation 15
4.1 Zertifikatantrag 15
4.2 Bearbeitung von Zertifikatanträgen 15
4.3 Zertifikatausstellung 15
4.4 Zertifikatakzeptanz 16
4.5 Verwendung des Schlüsselpaares und des Zertifikats 16
4.6 Zertifikaterneuerung / Re-Zertifizierung 17
4.7 Zertifikaterneuerung / Re-Key 17
4.8 Zertifikatmodifizierung 18
4.9 Widerruf und Suspendierung von Zertifikaten 18
4.10 Dienst zur Statusabfrage von Zertifikaten 19
4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatnehmer 20
4.12 Schlüsselhinterlegung und -wiederherstellung 20
5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen 20
6 Technische Sicherheitsmaßnahmen 20
7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen 20
8 Konformitätsprüfung 21
8.1 Frequenz und Umstände der Überprüfung 21
8.2 Identität des Überprüfers 21
8.3 Verhältnis von Prüfer zu Überprüftem 21

8.4 Überprüfte Bereiche 21
8.5 Mängelbeseitigung 21
8.6 Veröffentlichung der Ergebnisse 21
9 Rahmenvorschriften 22
9.1 Gebühren 22
9.2 Finanzielle Verantwortung 22
9.3 Vertraulichkeit von Geschäftsinformationen 22
9.4 Schutz personenbezogener Daten (Datenschutz) 22
9.5 Urheberrechte 23
9.6 Verpflichtungen 23
9.7 Gewährleistung 24
9.8 Haftungsbeschränkung 24
9.9 Haftungsfreistellung 24
9.10 Inkrafttreten und Aufhebung 24
9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern 25
9.12 Änderungen der Richtlinien 25
9.13 Konfliktbeilegung 25
9.14 Geltendes Recht 25
9.15 Konformität mit dem geltenden Recht 25
9.16 Weitere Regelungen 25
9.17 Andere Regelungen 26
10 Glossar 27
11 Referenzen 30

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

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

Um die internationale Zusammenarbeit mit anderen Zertifizierungsstellen zu ermöglichen, wird ferner eine englische Übersetzung von CP und CPS 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 Basic unterliegt.

In dieser CP der DFN-PKI sind die Rahmenbedingungen für die Ausstellung von Zertifikaten - entsprechend der internationalen Norm X.509 [X.509] - für das Sicherheitsniveau Basic festgelegt.

Diese CP beschreibt nicht die Vorgänge innerhalb der DFN-PKI, sondern nur welche Eigenschaften die Zertifikate haben und welche Vorgaben für das jeweilige Sicherheitsniveau gelten, um den Nutzern das Verständnis der DFN-PKI allgemein und speziell für das gewählte Sicherheitsniveau zu erleichtern. Detaillierte Informationen über Spezifikationen, über Prozesse der Zertifizierungsstellen und über technische Sicherheitsmaßnahmen sind dem jeweils zugehörigen CPS 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 ge-

setzlichen Regelungen widersprechen. Das diesem Sicherheitsniveau zugehörige CPS [CPS-BASIC] kann von nachgeordneten Zertifizierungsstellen innerhalb der DFN-PKI ergänzt werden, jedoch sind die infrastrukturellen, organisatorischen, personellen und technischen Maßnahmen (Abschnitt 5 und 6) als verbindlicher Maßstab anzusehen und dürfen in ihrer Qualität und Wirksamkeit nicht unterschritten werden.

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 wird durch den DFN-Verein realisiert. Der DFN-Verein kann bei der Erbringung der Zertifizierungsdienste durch Dienstleister unterstützt werden.

1.2 Identifikation des Dokuments

Identifikation

- **Titel: Zertifizierungsrichtlinie der Public Key Infrastruktur im Deutschen Forschungsnetz - Basic -**
- **Version: 1.1**
- **Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.2.1.1**
- **Zusammensetzung der OID:**

IANA	**1.3.6.1.4.1**
DFN-Verein	**22177**
PKI	**300**
Richtlinien	**1**
X.509	**1**
Basic	**2**
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 (PCA) der DFN-PKI ist in einem selbst-signierten Zertifikat (Wurzelzertifikat) enthalten. Alle Teilnehmer der DFN-PKI können dieses Zertifikat öffentlich abrufen und somit die Authentizität und Gültigkeit aller innerhalb der DFN-PKI ausgestellten Zertifikate überprüfen.

Die in diesem Dokument niedergelegte CP gilt für alle durch die PCA ausgestellten Zertifikate und für alle davon abgeleiteten Zertifikate innerhalb der DFN-PKI. Damit gibt diese CP den Handlungsrahmen und Mindestanforderungen für das ausgezeichnete Sicherheitsniveau vor. Die CP und das zugehörige CPS können durch nachgeordnete Zertifizierungsstellen den eigenen Bedürfnissen angepasst, jedoch keinesfalls abgeschwächt werden.

Die PCA zertifiziert für das ausgezeichnete Sicherheitsniveau ausschließlich nach dieser CP und dem zugehörigen CPS. Für jede nachgeordnete und direkt von der PCA zertifizierte Zer-

tifizierungsstelle muss eine Vereinbarung (Erklärung) zwischen einer juristischen Person und der PCA getroffen werden, in der die Einhaltung dieser CP zugesichert wird. Die Verfügbarkeit eigener Richtlinien bzw. deren Änderungen sind der zuständigen (ausstellenden) Zertifizierungsstelle mitzuteilen und bekannt zu geben. Dieses Prinzip ist für alle Ebenen der DFN-PKI bindend.

Die PCA zertifiziert ausschließlich Zertifikate von unmittelbar nachgeordneten Zertifizierungsstellen.

1.3.1.2 Zertifizierungsstellen (CA)

Alle innerhalb der DFN-PKI operierenden Zertifizierungsstellen unterhalb der PCA können Zertifikate für natürliche und juristische Personen ausstellen. Bei juristischen Personen können Zertifikate für Organisationseinheiten erstellt werden, z.B. für Zertifizierungs- und Registrierungsstellen oder Personen- bzw. Funktionsgruppen. Zertifikate für „Object-Signing" und Datenverarbeitungssysteme können für natürliche und juristische Personen ausgestellt werden.

Die Einhaltung der jeweiligen CP muss jeweils schriftlich gegenüber der übergeordneten CA zugesichert werden.

Bei größeren Organisationsstrukturen ist es möglich, dass innerhalb einer Organisation weitere nachgeordnete Zertifizierungsstellen etabliert werden, durch die eine Zertifizierung der jeweiligen Zertifikatnehmer erfolgt.

1.3.2 Registrierungsstellen

1.3.2.1 Ausgezeichnete Registrierungsstellen

Jeder Zertifizierungsstelle innerhalb der DFN-PKI ist eine ausgezeichnete Registrierungsstelle zugeordnet. Nur diese Registrierungsstellen dürfen zur Registrierung von unmittelbar nachgeordneten Zertifizierungs- und Registrierungsstellen eingesetzt werden. Die Überprüfung der Identität und Authentizität weiterer Zertifikatnehmer kann ebenso durchgeführt werden.

1.3.2.2 Registrierungsstellen (RA)

Alle Zertifizierungsstellen innerhalb der DFN-PKI haben die Möglichkeit, beliebig viele Registrierungsstellen für die lokale Überprüfung der Identität und Authentizität der Zertifikatnehmer zu benennen. Diese Registrierungsstellen dürfen jedoch nicht zur Registrierung von Zertifizierungs- und Registrierungsstellen eingesetzt werden.

Die Einhaltung der jeweiligen CP muss jeweils schriftlich gegenüber der zuständigen CA zugesichert werden. Ebenso sind die Benennung und Entbindung von RAs zu dokumentieren und zu kommunizieren.

1.3.3 Zertifikatnehmer

Zertifikate können an natürliche und juristische Personen vergeben werden, soweit dies der Satzung des DFN-Vereins entspricht.

1.3.4 Zertifikatprüfer

Unter Zertifikatprüfern sind natürliche Personen oder Organisationen zu verstehen, die unter Nutzung eines innerhalb der DFN-PKI ausgestellten Zertifikats die Identität eines Zertifikatnehmers überprüfen oder von diesem Informationen entgegennehmen oder diesem Informationen zukommen lassen. Ein Zertifikatprüfer kann – muss aber nicht – Teilnehmer der DFN-PKI sein.

1.3.5 Weitere Teilnehmer

Weitere Teilnehmer können natürliche oder juristische Personen sein, die in den Zertifizierungsprozess als Dienstleister eingebunden sind.

Bei Dienstleistern, die im Namen und Auftrag eines DFN-Anwenders tätig werden, liegt die Verantwortung bei dem beauftragenden DFN-Anwender.

Der Abschluss von Dienstleistungsabkommen mit einem Dienstleister oder die Entgegennahme und Akzeptanz von Leistungen eines Dienstleisters, der im eigenen Namen handelt, kann ausschließlich durch den DFN-Verein vorgenommen werden.

1.4 Anwendungsbereich

1.4.1 Geeignete Zertifikatnutzung

Die im Rahmen dieser CP ausgestellten Zertifikate können durch den Zertifikatnehmer für Authentifizierung, digitale Signatur und Verschlüsselung verwendet werden. Die Zertifikatnehmer sind selbst für die Benutzung in den Anwendungsprogrammen zuständig, sowie für die Prüfung, ob die damit möglichen Anwendungen den Sicherheitsanforderungen geeignet Rechnung tragen. Eine Installation von Anwendungsprogrammen durch die vom DFN-Verein betriebenen Zertifizierungsstellen findet nicht statt.

1.4.2 Untersagte Zertifikatnutzung

Grundsätzlich ist keine Zertifikatnutzung untersagt, jedoch ist die Zertifizierung weiterer, untergeordneter Zertifikate ausschließlich den Zertifizierungsstellen vorbehalten.

1.5 Verwaltung der Richtlinien

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**

Alle weiteren Regelungen sind dem CPS zu entnehmen

1.6 Definitionen und Abkürzungen

Siehe Glossar.

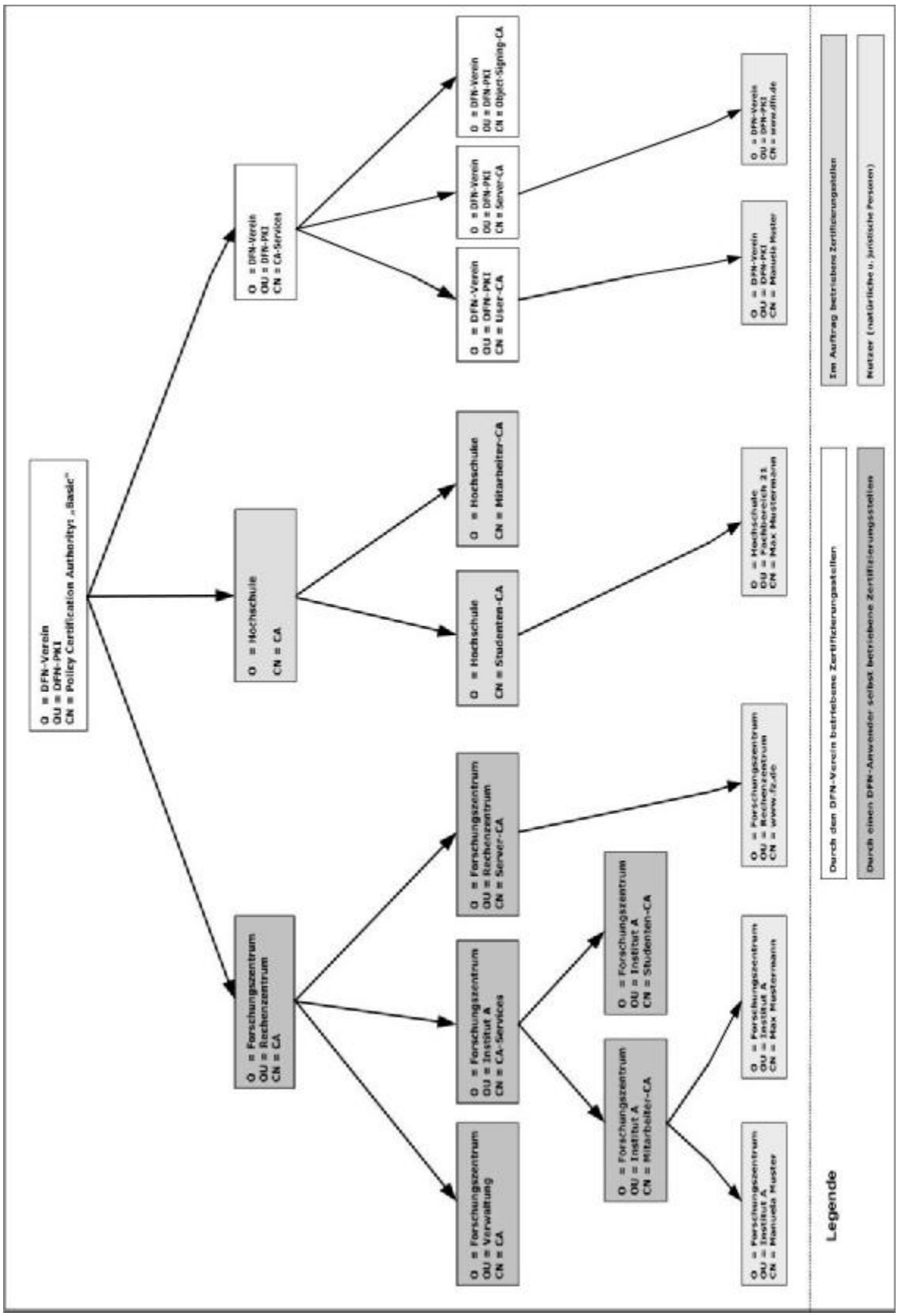

Abbildung 1: Zertifizierungshierarchie der DFN-PKI

2 Veröffentlichungen und Verzeichnisdienst

2.1 Verzeichnisdienst

Jede innerhalb der DFN-PKI operierende Zertifizierungsstelle muss Sorge tragen, dass Informationen zur Überprüfung der Gültigkeit von Zertifikaten bereitgestellt werden, die Online abrufbar sind.

Jede innerhalb der DFN-PKI operierende Zertifizierungsstelle sollte einen Dienst anbieten, mit dessen Hilfe die von der Zertifizierungsstelle herausgegebenen und zur Veröffentlichung freigegebenen Zertifikate abrufbar sind.

Details sind dem CPS zu entnehmen.

2.2 Veröffentlichung von Informationen

Jede innerhalb der DFN-PKI operierende Zertifizierungsstelle ist verpflichtet, folgende Informationen zur Verfügung zu stellen:

- **Das Wurzelzertifikat der DFN-PKI und dessen Fingerabdruck**
- **Zertifikate der Zertifizierungsstelle und der zuständigen Registrierungsstellen und deren Fingerabdrücke**
- **CP und zugehöriges CPS**

Darüber hinaus sollen Informationen über die DFN-PKI, über die korrekte Anwendung von Kryptographie und die Verwendung von Zertifikaten den Zertifikatnehmern zur Verfügung gestellt werden. Details der Bezugsadressen o.g. Informationen und ggf. weiterer Dienstleistungen sind dem CPS zu entnehmen.

2.3 Aktualisierung der Informationen

Eine Aktualisierung der Informationen zur Überprüfung der Gültigkeit von Zertifikaten muss regelmäßig erfolgen. Der Abstand zwischen zwei Aktualisierungen darf höchstens einen Monat betragen. Einzelheiten sind dem CPS zu entnehmen.

2.4 Zugang zu den Informationsdiensten

Der lesende Zugriff auf alle in den Abschnitten 2.1 und 2.2 aufgeführten Informationen sollte keiner Zugangskontrolle unterliegen. Schreibender Zugriff auf diese Informationen darf nur berechtigten Personen gewährt werden. Details sind dem CPS zu entnehmen.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensform

Es wird eine einheitliche Namenshierarchie verwendet. Alle innerhalb der DFN-PKI ausgestellten Zertifikate beinhalten eindeutige Namen (Distinguished Name, DN) entsprechend der Normenserie X.500. Ein DN enthält eine Folge von eindeutig kennzeichnenden Namensattributen, durch die alle Teilnehmer einer Hierarchie referenziert werden können.

Jede Zertifizierungsstelle vereinbart mit ihrer übergeordneten Zertifizierungsstelle einen eindeutigen Namensraum. Eine Zertifizierungsstelle darf bei der Ausstellung von Zertifikaten nur DNs verwenden, die in ihrem zugeordneten Namensraum liegen. Die Verantwortung für die Eindeutigkeit der Namen obliegt der ausstellenden Zertifizierungsstelle. Diese sollte die vergebenen Namensräume über einen Informationsdienst veröffentlichen.

Die Einzelheiten für die spezifischen Namensformen sind im CPS festgelegt.

3.1.2 Aussagekräftigkeit von Namen

Der DN muss den Zertifikatnehmer eindeutig identifizieren und in einer für Menschen verständlichen Form vorliegen. Bei der Namensvergabe gelten grundsätzlich die folgenden Regelungen:

- **Zertifikate dürfen nur auf einen zulässigen Namen des Zertifikatnehmers ausgestellt werden.**
- **Zertifikate für eine Organisationseinheit oder für ein Datenverarbeitungssystem müssen als solche erkennbar sein.**
- **Werden Zertifikate für Zertifikatnehmer ausgestellt, die nicht einem DFN-Anwender angehören und die nicht im Namen und Auftrag eines DFN-Anwenders handeln (siehe Abschnitt 1.3.3), muss dies im DN erkennbar sein.**
- **Bei der Vergabe von Namen für Pseudonyme muss eine Verwechslung mit natürlichen und juristischen Personen oder Bezeichnungen von Organisationseinheiten ausgeschlossen werden. Ebenso dürfen keine DNS-Namen, IP-Adressen oder andere innerhalb der DFN-PKI benutzte Syntaxelemente verwendet werden. Ein Pseudonym darf keinen beleidigenden oder anzüglichen Inhalt enthalten. Diskriminierungen sind in jeglicher Form unzulässig.**
- **Bei der Vergabe von Namen für Organisationseinheiten muss eine Verwechslung mit natürlichen oder juristischen Personen ausgeschlossen werden. Ebenso dürfen keine DNS-Namen, IP-Adressen oder andere innerhalb der DFN-PKI benutzten Syntaxelemente verwendet werden.**
- **Bei der Vergabe von Zertifikaten für Datenverarbeitungssysteme, sollte für den Namen grundsätzlich der voll qualifizierte Domain-Name verwendet werden. Die Verwendung optionaler Attribute ist möglich.**

Darüber hinaus wird jedem Zertifikat eine eindeutige Seriennummer zugeordnet, welche eine eindeutige und unveränderliche Zuordnung zum Zertifikatnehmer ermöglicht. Die Einzelheiten sind im CPS festgelegt.

3.1.3 Pseudonymität / Anonymität

Auf Verlangen einer natürlichen Person kann anstelle des Namens im Zertifikat ein Pseudonym aufgeführt werden, dieses ist bereits im CN eindeutig kenntlich zu machen. Einzelheiten regelt das CPS. Für die Eindeutigkeit von Pseudonymen gelten weiterhin auch die Regelungen unter 3.1.5.

Die Identitätsprüfung erfolgt immer entsprechend den Regelungen unter 3.2. Anonyme Zertifikate sind daher nicht möglich.

Die Identität eines Zertifikatnehmers muss auf richterliche Anordnung aufgedeckt werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Der zu verwendende Zeichensatz und die Substitutionsregelungen für Sonderzeichen sind dem CPS zu entnehmen.

3.1.5 Eindeutigkeit von Namen

Vor der Zertifizierung muss die Korrektheit und Eindeutigkeit des angegebenen Namens von der zuständigen Zertifizierungsstelle überprüft werden. Der DN eines Zertifikatnehmers muss eindeutig sein und darf nicht an unterschiedliche Zertifikatnehmer vergeben werden. Nur wenn ein Zertifikatnehmer mehrere Zertifikate mit disjunkter Schlüsselnutzung besitzt, kann ein DN mehrmals vorkommen. Seriennummern in Bezug zu einer ausstellenden CA sind jedoch uneingeschränkt eindeutig.

Bei Namensgleichheit gilt grundsätzlich das Prinzip: „wer zuerst kommt, wird zuerst bedient". Bei Streitigkeiten entscheidet die zuständige Zertifizierungsstelle.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Sofern sich der DN auf dem Zertifikat explizit auf eine natürliche Person bezieht, ist eine Anerkennung von Warenzeichen nicht relevant. In allen anderen Fällen liegt es in der Verantwortung des Zertifikatnehmers, dass die Namenswahl keine Warenzeichen, Markenrechte usw. verletzt. Die Zertifizierungsstellen sind nicht verpflichtet, solche Rechte zu überprüfen. Allein der Zertifikatnehmer ist für solche Überprüfungen verantwortlich. Falls eine Zertifizierungsstelle über eine Verletzung solcher Rechte informiert wird, wird das Zertifikat widerrufen.

3.2 Identitätsüberprüfung bei Neuantrag

In Abhängigkeit vom Verwendungsweck des Zertifikats, gelten für die Identitätsüberprüfung eines Zertifikatnehmers die folgenden Regeln:

- **Natürliche Personen: Damit die Angaben in einem Zertifikat durch eine Zertifizierungsstelle beglaubigt werden können, muss die Identität und Authentizität einer natürlichen Person mittels geeigneter Verfahren durch die ausstellende Zertifizierungsstelle bzw. durch eine zuständige Registrierungsstelle überprüft werden. Die im Rahmen dieser CP akzeptierten Verfahren sind in Abschnitt 3.2.3 aufgeführt.**
- **Juristische Personen: Ist der Zertifikatnehmer eine juristische Person, sind bei der Registrierung folgende Sachverhalte zu verifizieren:**
  - **a) Die Existenz und Identität der juristischen Person, z.B. durch Vorlage eines aussagefähigen Dokuments.**
  - **b) Nachweis der Berechtigung zum Leistungsempfang (siehe 3.2.2).**
  - **c) Die Akkreditierung einer handlungsberechtigten Person oder eines beauftragten Dienstleisters durch die beantragende juristische Person (siehe 3.2.5).**
  - **d) Authentifizierung der handlungsberechtigten Person. Die Überprüfung der Identität und Authentizität einer handlungsberechtigten Person erfolgt anhand der Regelungen nach Abschnitt 3.2.3 (mit Ausnahme von c).**

Handelt es sich bei dem Zertifikatnehmer um eine Zertifizierungsstelle oder Registrierungsstelle, ist eine Überprüfung der Identität und Authentizität immer nach Abschnitt 3.2.3 a) notwendig.

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, sofern die Schlüsselerzeugung nicht bei der Zertifizierungsstelle stattfindet. Die entsprechenden Verfahren werden im CPS beschrieben.

3.2.2 Authentifizierung einer Organisation

Der DFN-Verein stellt der PCA ein Verfahren bereit, mit dem die Berechtigung einer Organisation zum Leistungsempfang verifiziert werden kann. Die Details sind dem CPS zu entnehmen.

3.2.3 Authentifizierung einer natürlichen Person

Für die Identitätsprüfung einer natürlichen Person sind folgende Verfahren anwendbar:

a) Der Zertifikatnehmer erscheint persönlich bei der ausstellenden Zertifizierungsstelle oder einer zuständigen Registrierungsstelle, wobei ein Mitarbeiter der CA oder RA die Identitätsprüfung anhand eines amtlichen Ausweispapiers mit Lichtbild (Personalausweis oder Reisepass und Meldebescheinigung) durchführt.

b) Die Authentifizierung einer natürlichen Person wird durch einen geeigneten Dienstleister vorgenommen, der eine persönliche Identitätsprüfung anhand eines amtlichen Ausweispapiers mit Lichtbild (Personalausweis oder Reisepass und Meldebescheinigung) durchführt und entsprechend dokumentiert. Die genutzte Dienstleistung muss entweder über eine Konformitätsbestätigung für die Umsetzung von Sicherheitskonzepten durch eine von der RegTP (Regulierungsbehörde für Telekommunikation und Post) anerkannten Prüf- und Bestätigungsstelle verfügen oder ein konformes Verhalten muss durch vertragliche Regelungen verpflichtend gemacht werden.

c) Die Authentifizierung einer natürlichen Person kann bei entsprechenden Voraussetzungen anhand der postalischen Adresse (Erstwohnsitz) erfolgen. Die Korrektheit der Adresse muss durch geeignete Maßnahmen verifiziert werden. Eine Anonymisierung der postalischen Adresse, z.B. die Verwendung von Postfächern oder die Hinterlegung auf dem Postamt (postlagernd), ist dabei nicht zulässig. Details der Verfahren sind dem CPS zu entnehmen.

Verfügt die beantragende Person über ein gültiges Zertifikat, so kann die Beantragung weiterer Zertifikate für diese Person auch durch die Übersendung eines verschlüsselten und signierten Antrags erfolgen, sofern sich die Identität der Person nicht geändert hat.

Voraussetzung für diese Art der Antragstellung ist, dass seit dem Erstantrag des gültigen Zertifikats nicht mehr als zwei Jahre vergangen sind und das bei der Identifizierung vorgelegte Ausweisdokument noch gültig ist.

3.2.4 Nicht überprüfte Informationen

Es werden die Informationen überprüft, die je nach Art der Authentifizierung für die Identitätsprüfung erforderlich sind (Abschnitt 3.2.3). Darüber hinaus werden keine weiteren Informationen überprüft.

3.2.5 Unterschriftenvollmacht

Die Akkreditierung einer handlungsberechtigten Person durch die beantragende Organisation muss in schriftlicher Form oder durch ein adäquates Verfahren durch eine zur Unterschrift bevollmächtigte Person erfolgen.

Die Akkreditierung eines beauftragten Dienstleisters durch die beantragende Organisation muss in schriftlicher Form oder durch ein adäquates Verfahren durch eine zur Unterschrift bevollmächtigte Person erfolgen. Der beauftragte Dienstleister muss seinerseits wie in Abschnitt 3.2 geregelt eine handlungsberechtigte Person akkreditieren.

Überprüfungen von Unterschriftenvollmachten liegen im Verantwortungsbereich der Organisation, die eine Akkreditierung vornimmt.

Weitere Details sind dem CPS zu entnehmen.

3.2.6 Cross-Zertifizierung

Um die Anbindung an andere Zertifizierungshierarchien zu erlauben, besteht für die PCA die Möglichkeit der Cross-Zertifizierung mit Zertifizierungsstellen innerhalb und außerhalb der DFN-PKI. Dies gilt grundsätzlich auch für die der PCA nachgeordneten Zertifizierungsstellen. Diese müssen jedoch eine Cross-Zertifizierung mit Zertifizierungsstellen außerhalb der DFN-PKI bei der PCA genehmigen lassen.

Der Vorgang der Cross-Zertifizierung unterscheidet sich dabei für die PCA und andere Zertifizierungsstellen innerhalb der DFN-PKI nicht. Vor einer Cross-Zertifizierung haben sich die Verantwortlichen mit den Richtlinien der jeweils anderen Seite vertraut zu machen. Wenn eine hinreichende Richtlinien-Äquivalenz hinsichtlich des Sicherheitsniveaus gegeben ist, können die Richtlinien akzeptiert und eine Cross-Zertifizierung vorgenommen werden.

Die Cross-Zertifizierung bezieht sich immer auf die momentan gültige CP einer Zertifizierungsstelle. Wird diese grundlegend geändert, ist eine erneute Cross-Zertifizierung erforderlich. Änderungen sind daher der jeweils anderen Seite mitzuteilen. Der Bedarf für eine erneute Cross-Zertifizierung ist bei jeder Änderung einer CP zu überprüfen. Der Nachweis zur Berechtigung zum Leistungsempfang entfällt.

Eine Cross-Zertifizierung wird wie die Zertifizierung einer CA behandelt, der Nachweis zur Berechtigung zum Leistungsempfang entfällt in diesem Fall. Nach der Zertifizierung veröffentlicht die Zertifizierungsstelle das erteilte Cross-Zertifikat, welches den Public Key der anderen Zertifizierungsstelle enthält. Ein Cross-Zertifikat darf keine längere Gültigkeitsdauer als die regulären Zertifikate der beteiligten Zertifizierungsstellen besitzen.

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

3.3.1 Routinemäßige Zertifikaterneuerung

Eine Zertifikaterneuerung setzt voraus, dass der Zertifikatnehmer über ein gültiges Zertifikat der zuständigen Zertifizierungsstelle verfügt. Darüber hinaus muss der Zertifikatnehmer gegenüber der zuständigen Zertifizierungsstelle vor der Ausstellung eines neuen Zertifikats den Besitz des privaten Schlüssels nachweisen (siehe 3.2.1) und die Gültigkeit der Angaben im Zertifikat bestätigen.

3.3.2 Zertifikaterneuerung nach dem Widerruf

Nach dem Widerruf eines Zertifikats erfolgt keine Zertifikaterneuerung, es ist ein neues Zertifikat zu beantragen. Es gelten die Regelungen nach Abschnitt 3.2.

3.4 Identifizierung und Authentifizierung bei einem Widerruf

Um ein Zertifikat bei der ausstellenden Zertifizierungsstelle oder einer zuständigen Registrierungsstelle widerrufen zu können, muss dem Zertifikatnehmer ein adäquates Verfahren angeboten werden. Der Widerruf eines Zertifikats kann telefonisch unter Angabe der mit der CA oder RA vereinbarten Autorisierungsinformation oder handschriftlich erfolgen. Unter bestimmten Voraussetzungen kann ein Widerruf auch elektronisch erfolgen, die Details sind dem CPS zu entnehmen.

4 Ablauforganisation

4.1 Zertifikatantrag

4.1.1 Wer kann ein Zertifikat beantragen

Innerhalb der DFN-PKI können Zertifikate an Zertifikatnehmer ausgestellt werden, wenn die in Abschnitt 1.3.3 aufgeführten Voraussetzungen gegeben sind. Der PCA nachgeordnete Zertifizierungsstellen können den Kreis der berechtigten Zertifikatnehmer weiter eingrenzen.

4.1.2 Registrierungsprozess

Ein Zertifikat kann durch eine Zertifizierungsstelle erst erzeugt werden, wenn der Registrierungsprozess bei einer zuständigen Registrierungsstelle oder Zertifizierungsstelle erfolgreich abgeschlossen wurde. Die Dokumentation des Registrierungsprozesses bei natürlichen Personen beinhaltet zumindest:

- **Zertifikatantrag**
- **Erklärung über den alleinigen Besitz des privaten Schlüssels, sofern die Schlüsselerzeugung nicht bei der Zertifizierungsstelle stattfindet.**

Bei juristischen Personen müssen zusätzliche Informationen oder Dokumente entsprechend den Regelungen nach Abschnitt 3.2 (Absatz a – c) vorliegen.

4.2 Bearbeitung von Zertifikatanträgen

4.2.1 Durchführung der Identifikation und Authentifizierung

Die zuständige Registrierungs- oder Zertifizierungsstelle führt die Identifikation und Authentifizierung eines Zertifikatnehmers nach den im Abschnitt 3.2 genannten Verfahren durch.

4.2.2 Annahme oder Abweisung von Zertifikatanträgen

Der Zertifizierungsantrag wird von der zuständigen Registrierungs- oder Zertifizierungsstelle angenommen, wenn die folgenden Kriterien erfüllt wurden:

- **Vorlage aller notwendigen Dokumente (siehe Abschnitt 4.1.2)**
- **Zahlung der ggf. festgelegten Gebühr (siehe Abschnitt 9.1)**

Nach erfolgreicher Prüfung der o.g. Kriterien und nach Durchführung der Identifikation und Authentifizierung wird der Zertifizierungsantrag durch die ausstellende Zertifizierungsstelle weiter bearbeitet.

Sollte die Prüfung der o.g. Kriterien oder die Identifikation und Authentifizierung eines Zertifikatnehmers nicht erfolgreich sein, wird der Zertifizierungsantrag nicht bearbeitet. Der Sachverhalt ist dem Zertifikatnehmer unter Angaben von Gründen mitzuteilen.

4.2.3 Bearbeitungsdauer

Die Bearbeitungsdauer ist dem CPS zu entnehmen.

4.3 Zertifikatausstellung

Nach Eingang und erfolgreicher Prüfung (siehe 4.3.1) eines Zertifizierungsantrags wird durch die Zertifizierungsstelle ein Zertifikat ausgestellt und der Zertifikatnehmer über diesen Vorgang informiert (siehe 4.3.2).

4.3.1 Weitere Prüfungen der Zertifizierungsstelle

Die formalen Voraussetzungen für die Ausstellung eines Zertifikats werden durch die Zertifizierungsstelle in angemessener Weise überprüft. Weitere Überprüfungen finden nicht statt.

4.3.2 Benachrichtigung des Antragstellers

Nach der Zertifikatausstellung wird dem Zertifikatnehmer in geeigneter Weise das ausgestellte Zertifikat durch die Zertifizierungsstelle übermittelt bzw. über dessen Ausstellung informiert. Werden nicht im Zertifikat enthaltene persönliche Angaben oder Autorisierungsinformationen übertragen, so sind diese angemessen zu schützen. Die Verfahren sind dem CPS zu entnehmen.

4.4 Zertifikatakzeptanz

Der Zertifikatnehmer ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der ausstellenden Zertifizierungsstelle nach Erhalt zu verifizieren.

4.4.1 Annahme des Zertifikats

Ein Zertifikat wird durch den Zertifikatnehmer akzeptiert, wenn

- **das Zertifikat verwendet wird oder**
- **wenn innerhalb eines im CPS festgelegten Zeitraums kein Widerspruch erfolgt.**

Fehlerhaft ausgestellte Zertifikate hat die ausstellende Zertifizierungsstelle unverzüglich zu widerrufen.

4.4.2 Veröffentlichung des Zertifikats

Es gelten die Regelungen aus Abschnitt 2.1.

4.4.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist grundsätzlich nicht vorgesehen, ggf. abweichende Regelungen sind dem CPS zu entnehmen.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Der Anwendungsbereich der im Rahmen dieser CP ausgestellten Zertifikate ist dem Abschnitt 1.4 zu entnehmen.

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatnehmer

Durch Annahme des Zertifikats versichert der Zertifikatnehmer allen Teilnehmern der DFN-PKI und allen Parteien, die sich auf die Vertrauenswürdigkeit der in dem Zertifikat enthaltenden Informationen verlassen, dass

- **ein grundlegendes Verständnis der Anwendung und des Einsatzes von Zertifikaten besteht,**
- **sämtliche Angaben und Erklärungen des Zertifikatnehmers in Bezug auf die im Zertifikat enthaltenden Informationen der Wahrheit entsprechen,**
- **der private Schlüssel geschützt aufbewahrt wird,**
- **keiner unbefugten Person Zugang zu dem privaten Schlüssel gewährt wird,**
- **das Zertifikat ausschließlich in Übereinstimmung mit dieser CP eingesetzt wird,**
- **das Zertifikat unverzüglich widerrufen wird, wenn die Angaben des Zertifikats nicht mehr stimmen oder der private Schlüssel abhanden kommt, gestohlen oder möglicherweise kompromittiert wurde und**

- **die Zertifizierung weiterer Zertifikate nur durch Zertifizierungsstellen erfolgt.**

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Zertifikatprüfer

Jeder, der ein Zertifikat, welches im Rahmen dieser CP ausgestellt wurde, zur Überprüfung einer Signatur oder für die Zwecke der Authentifizierung oder Verschlüsselung verwendet, sollte

- **ein grundlegendes Verständnis der Anwendung und des Einsatzes von Zertifikaten besitzen,**
- **vor der Nutzung eines Zertifikats dessen Gültigkeit überprüfen und**
- **das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit dieser CP einsetzen.**

4.6 Zertifikaterneuerung / Re-Zertifizierung

Bei einer Re-Zertifizierung wird dem Zertifikatnehmer durch die zuständige Zertifizierungsstelle ein neues Zertifikat unter Beibehaltung des alten Schlüsselpaars ausgestellt, sofern die kryptographischen Verfahren dem zu dem jeweiligen Zeitpunkt geltenden CPS genügen, die im Zertifikat enthaltenen Informationen unverändert bleiben und kein Verdacht auf Kompromittierung des privaten Schlüssels vorliegt. Das alte Zertifikat wird nach Ausstellung des neuen Zertifikats widerrufen.

4.6.1 Gründe für eine Zertifikaterneuerung

Eine Zertifikaterneuerung kann nur dann beantragt werden, wenn die Gültigkeit des Zertifikats abläuft.

4.6.2 Wer kann eine Zertifikaterneuerung beantragen

Eine Zertifikaterneuerung wird grundsätzlich durch den Zertifikatnehmer beantragt, es obliegt der zuständigen Zertifizierungsstelle, ob sie eine Zertifikaterneuerung aktiv unterstützt. Entsprechende Prozesse sind dem jeweiligen CPS zu entnehmen.

4.6.3 Ablauf der Zertifikaterneuerung

Der Ablauf der Zertifikaterneuerung entspricht den Regelungen unter 4.3, für die Identifizierung und Authentifizierung bei der Re-Zertifizierung gelten die Regelungen gemäß Abschnitt 3.3.1.

4.6.4 Benachrichtigung des Zertifkatsnehmers

Es gelten die Regelungen gemäß Abschnitt 4.3.2.

4.6.5 Annahme einer Zertifikaterneuerung

Es gelten die Regelungen gemäß Abschnitt 4.4.1.

4.6.6 Veröffentlichung einer Zertifikaterneuerung

Es gelten die Regelungen gemäß Abschnitt 4.4.2.

4.6.7 Benachrichtigung weiterer Instanzen über eine Zertifikaterneuerung

Es gelten die Regelungen gemäß Abschnitt 4.4.3.

4.7 Zertifikaterneuerung / Re-Key

Es gelten sinngemäß die Regelungen aus dem Abschnitt 4.6. Bei einem Re-Key wird jedoch ein neues Schlüsselpaar verwendet.

4.8 Zertifikatmodifizierung

Eine Zertifikatsmodifizierung kann vorgenommen werden, wenn sich die im Zertifikat enthaltenen Informationen verändern. Sofern sich die Identität des Zertifikatnehmers geändert hat, ist wie bei einem Neuantrag zu verfahren. Ansonsten können sinngemäß die Regelungen aus den Abschnitten 4.6 und 4.7 zur Anwendung kommen. Das alte Zertifikat wird nach Ausstellung des neuen Zertifikats widerrufen.

4.9 Widerruf und Suspendierung von Zertifikaten

In diesem Abschnitt werden die Umstände erläutert, unter denen ein Zertifikat widerrufen werden muss. Eine Suspendierung (zeitliche Aussetzung) von Zertifikaten wird nicht vorgenommen. Einmal widerrufene Zertifikate können nicht erneuert oder verlängert werden.

4.9.1 Gründe für einen Widerruf

Zertifikate müssen von der zuständigen Zertifizierungsstelle widerrufen werden, wenn mindestens einer der folgenden Gründe bekannt wird:

- **Ein Zertifikat enthält Angaben, die nicht mehr gültig sind.**
- **Der private Schlüssel des Zertifikatnehmers wurde geändert, verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.**
- **Der Zertifikatnehmer hat seine Berechtigungsgrundlage (siehe 1.3.3) verloren.**
- **Der Zertifikatnehmer hält die CP nicht ein.**
- **Die zuständige Zertifizierungsstelle bzw. eine Registrierungsstelle hält die CP oder das CPS nicht ein.**
- **Der Zertifikatnehmer benötigt kein Zertifikat mehr.**
- **Der Zertifizierungsbetrieb wird eingestellt.**

4.9.2 Wer kann widerrufen

Zertifikate können grundsätzlich nur von der ausstellenden Zertifizierungsstelle widerrufen werden. Sofern dies nicht durch das CPS eingeschränkt wird, kann jeder Zertifikatnehmer von der Zertifizierungsstelle, die sein Zertifikat erstellt hat, ohne Angabe von Gründen verlangen, dass diese ein für ihn ausgestelltes Zertifikat widerruft. Verfahren für einen Zertifikatwiderruf sind dem zugehörigen CPS zu entnehmen. Voraussetzung für die Akzeptanz eines Zertifikatwiderrufs ist eine erfolgreiche Identifizierung und Authentifizierung des Zertifikatnehmers entsprechend Abschnitt 3.4.

4.9.3 Ablauf eines Widerrufs

Sind die Voraussetzungen für einen Zertifikatwiderruf erfüllt, wird das Zertifikat gesperrt.

4.9.4 Fristen für den Zertifikatnehmer

Der Zertifikatnehmer sollte unverzüglich die zuständige Zertifizierungsstelle benachrichtigen und den Widerruf des eigenen Zertifikats veranlassen, wenn Gründe (siehe 4.9.1) für einen Widerruf vorliegen.

4.9.5 Fristen für die Zertifizierungsstelle

Eine Zertifizierungsstelle sollte unverzüglich einen Auftrag für einen Zertifikatwiderruf bearbeiten, wenn die Voraussetzungen gegeben sind.

4.9.6 Anforderungen zur Kontrolle der CRL durch den Zertifikatprüfer

Es gelten die Regelungen gemäß Abschnitt 4.5.2.

4.9.7 Veröffentlichungsfrequenz für CRLs

Die Veröffentlichungsfrequenz für eine CRL ist dem zugehörigen CPS zu entnehmen.

4.9.8 Maximale Latenzzeit für CRLs

Die maximale Latenzzeit für eine CRL ist dem zugehörigen CPS zu entnehmen.

4.9.9 Verfügbarkeit von Online-Widerrufs/Status-Überprüfungsverfahren

Jede Zertifizierungsstelle muss ein Online-Verfahren anbieten, mit dem die Gültigkeit eines Zertifikats überprüft werden kann. Es müssen dabei alle Zertifikate erfasst werden, die von der Zertifizierungsstelle ausgestellt worden sind. Details sind dem zugehörigen CPS zu entnehmen.

4.9.10 Anforderungen an Online-Widerrufs/Status-Überprüfungsverfahren

Vor jeder Nutzung eines Zertifikats sollte dessen Gültigkeit überprüft werden, die Standards sind den Abschnitten 7.2 (CRL Profile) und 7.3 (OCSP Profile) des CPS zu entnehmen.

4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung

Derzeit werden keine anderen Verfahren zur Widerrufsbekanntmachung eingesetzt.

4.9.12 Kompromittierung von privaten Schlüsseln

Bei einer Kompromittierung des privaten Schlüssels ist das entsprechende Zertifikat unverzüglich zu widerrufen. Bei einer Kompromittierung des privaten Schlüssels einer Zertifizierungsstelle werden alle von ihr ausgestellten Zertifikate gesperrt.

4.9.13 Gründe für eine Suspendierung

Eine Suspendierung von Zertifikaten wird nicht unterstützt.

4.9.14 Wer kann suspendieren

Entfällt.

4.9.15 Ablauf einer Suspendierung

Entfällt.

4.9.16 Begrenzung der Suspendierungsperiode

Entfällt.

4.10 Dienst zur Statusabfrage von Zertifikaten

Sofern dieser Dienst von einer Zertifizierungsstelle angeboten wird, sind die Details zum Verfahren, Verfügbarkeit und dessen Merkmale dem zugehörigen CPS zu entnehmen.

4.10.1 Verfahrensmerkmale

Die Verfahrensmerkmale sind dem CPS zu entnehmen.

4.10.2 Verfügbarkeit des Dienstes

Die Angaben über die Verfügbarkeit des Dienstes sind dem CPS zu entnehmen.

4.10.3 Optionale Merkmale

Die optionalen Dienstmerkmale sind dem CPS zu entnehmen.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatnehmer

Die Dauer des Vertragsverhältnisses ergibt sich aus der im Zertifikat angegebenen Gültigkeitsdauer.

Die Aufbewahrungsdauer von Dokumenten und Zertifikaten entspricht mindestens der Gültigkeitsdauer des Zertifikats der Zertifizierungsstelle, mit dem das Zertifikat des Zertifikatnehmers erstellt wurde, zuzüglich eines Jahres.

4.12 Schlüsselhinterlegung und -wiederherstellung

Wenn die Dienstleistungen Schlüsselhinterlegung und –wiederherstellung (Key-Escrow and Recovery) von einer Zertifizierungsstelle oder durch einen Dienstleister angeboten werden, so sind die Referenzen der entsprechenden Richtlinien und Verfahrensbeschreibungen anzugeben.

Das „nonRepudiation“ Flag darf in einem Zertifikat nur gesetzt werden, wenn keine Wiederherstellung des privaten Schlüssels durch die Zertifizierungsstelle oder einen Dritten möglich ist. Zertifizierungsstellen, die Zugriff auf den privaten Schlüssel eines Zertifikatnehmers haben und das „nonRepudiation“ Flag in dessen Zertifikat setzen, müssen sicherstellen, dass der private Schlüssel auf Seiten der Zertifizierungsstelle nachhaltig gelöscht wird.

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Die PCA stellt diese Dienstleistungen ihren Zertifikatnehmern im Rahmen dieser CP nicht zur Verfügung. Nachgeordneten Zertifizierungsstellen steht es frei, ihren Zertifikatnehmern die Dienstleistungen Schlüsselhinterlegung und -wiederherstellung anzubieten. Die Merkmale der Dienstleistungen sind dem zugehörigen CPS zu entnehmen.

4.12.2 Richtlinien und Praktiken zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung

Die PCA stellt diese Dienstleistungen ihren Zertifikatnehmern im Rahmen dieser CP nicht zur Verfügung. Nachgeordneten Zertifizierungsstellen steht es frei, ihren Zertifikatnehmern die Dienstleistungen zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung anzubieten. Die Merkmale der Dienstleistungen sind dem zugehörigen CPS zu entnehmen.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen sind dem CPS zu entnehmen. Einzelne Bereiche können in eigenständigen Dokumenten vorliegen, die nicht zwingend veröffentlicht werden.

6 Technische Sicherheitsmaßnahmen

Technische Sicherheitsmaßnahmen sind dem CPS zu entnehmen.

7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen sind im CPS festgelegt.

8 Konformitätsprüfung

Jede Zertifizierungsstelle innerhalb der DFN-PKI ist verpflichtet, dass alle ihre Abläufe der CP und dem zugehörigen CPS entsprechen. Jeder Zertifizierungsstelle ist vorbehalten, alle ihr nachgeordneten Zertifizierungs- und Registrierungsstellen auf die Einhaltung der entsprechenden CP hin zu überprüfen. Die Überprüfung der PCA erfolgt durch einen beauftragten Dritten. Werden die Leistungen der PCA von einem Dienstleister erbracht, kann die Konformitätsprüfung durch den DFN-Verein vorgenommen werden.

8.1 Frequenz und Umstände der Überprüfung

Frequenz oder Umstände, die zu einer Überprüfung führen können, werden durch die zuständige Zertifizierungsstelle festgelegt.

8.2 Identität des Überprüfers

Die zuständige Zertifizierungsstelle kann selbst die Einhaltung der Richtlinien der ihr nachgeordneten Zertifizierungs- und Registrierungsstellen überprüfen. Eine Konformitätsprüfung kann aber auch durch Dritte vorgenommen werden.

8.3 Verhältnis von Prüfer zu Überprüftem

Das Verhältnis von Prüfer zu Überprüftem ergibt sich aus Abschnitt 8.2. Eine Selbstüberprüfung ist nicht zulässig.

8.4 Überprüfte Bereiche

Die von einer Überprüfung betroffenen Bereiche werden jeweils durch die zuständige Zertifizierungsstelle festgelegt. Für Umstände, die zwingend eine Überprüfung notwendig machen, können bestimmte Bereiche von vorne herein festgelegt werden.

8.5 Mängelbeseitigung

Aufgedeckte Mängel müssen in Abstimmung zwischen der zuständigen Zertifizierungsstelle und der überprüften Zertifizierungs- bzw. Registrierungsstelle behoben werden.

8.6 Veröffentlichung der Ergebnisse

Wenn sich der DFN-Verein zur Erbringung seiner Dienstleistungen eines Dienstleisters bedient, werden dem DFN-Verein von diesem Dienstleister regelmäßig Berichte vorgelegt. Eine allgemeine Veröffentlichung der Prüfungsergebnisse ist nicht vorgesehen.

9 Rahmenvorschriften

9.1 Gebühren

Die Gebühren für Dienstleistungen, die durch die vom DFN-Verein betriebenen Zertifizierungsstellen erbracht werden, sind einer Preisliste zu entnehmen. Diese kann bei der in Abschnitt 1.5 angegebenen Kontaktadresse abgerufen werden. Zusätzliche Leistungen, die nicht durch die Preisliste abgedeckt sind, können gesondert in Rechnung gestellt werden.

9.2 Finanzielle Verantwortung

9.2.1 Versicherungsschutz

Keine Angabe.

9.2.2 Vermögenswerte

Keine Angabe.

9.2.3 Versicherungsschutz für Zertifikatnehmer

Ein Versicherungsschutz für Zertifikatnehmer ist nicht gegeben.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter 9.3.2 fallen, werden als vertrauliche Informationen eingestuft. Zu diesen Informationen zählen u.a. Geschäftspläne, Vertriebsinformationen, Informationen über Geschäftspartner und ebenso alle Informationen, die beim Registrierungsprozess zur Kenntnis gekommen sind.

9.3.2 Nicht vertraulich zu behandelnde Daten

Jegliche Informationen, die in den herausgegebenen Zertifikaten und Widerrufslisten explizit (z.B. E-Mail-Adresse) oder implizit (z.B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Jede innerhalb der DFN-PKI operierende Zertifizierungsstelle trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten dürfen im Rahmen der Diensterbringung an Dritte nur weitergegeben werden, wenn zuvor eine Vertraulichkeitserklärung unterzeichnet wurde und die mit den Aufgaben betrauten Mitarbeiter auf Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet wurden.

9.4 Schutz personenbezogener Daten (Datenschutz)

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Die innerhalb der DFN-PKI operierenden Zertifizierungs- und Registrierungsstellen müssen zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten. Dies muss in Übereinstimmung mit den deutschen Datenschutzgesetzen und § 14 des Deutschen Signaturgesetzes [SigG] geschehen. Darüber hinaus gelten alle Regelungen aus Abschnitt 9.3.

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.1. analog.

9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.2. analog.

9.4.4 Verantwortlicher Umgang mit personenbezogenen Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.3. analog.

9.4.5 Nutzung personenbezogener Daten

Der Zertifikatnehmer stimmt der Nutzung von personenbezogenen Daten durch eine Zertifizierungsstelle zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden (dazu Abschnitt 9.4.3).

9.4.6 Offenlegung bei gerichtlicher Anordnung oder in Rahmen einer gerichtlichen Beweisführung

Alle innerhalb der DFN-PKI operierenden Zertifizierungsstellen unterliegen dem Recht der Bundesrepublik Deutschland und müssen vertrauliche und personenbezogene Informationen an staatliche Organe beim Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen freigeben.

9.4.7 Andere Umstände einer Veröffentlichung

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

9.5 Urheberrechte

Der DFN-Verein ist Urheber der folgenden Dokumente:

- **Vorliegende CP**
- **Dazugehöriges CPS**

Der DFN-Verein räumt den nachgeordneten Zertifizierungsstellen und den Zertifikatnehmern das Recht ein, die genannten Dokumente unverändert an Dritte weiter zu geben. Weitergehende Rechte werden nicht eingeräumt. Insbesondere ist die Weitergabe veränderter Fassungen und die Überführung in maschinenlesbare oder andere veränderbare Formen der elektronischen Speicherung, auch auszugsweise, ohne Zustimmung des DFN-Vereins nicht zulässig.

9.6 Verpflichtungen

9.6.1 Verpflichtung der Zertifizierungsstellen

Jede innerhalb der DFN-PKI operierende Zertifizierungsstelle verpflichtet sich, alle im Rahmen dieser CP und dem jeweils zugehörigen CPS beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.2 Verpflichtung der Registrierungsstellen

Jede innerhalb der DFN-PKI operierende Zertifizierungsstelle und die in ihren Namen agierenden Registrierungsstellen verpflichten sich, alle in dieser CP und dem jeweils zugehörigen CPS beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.3 Verpflichtung des Zertifikatnehmers

Es gelten die Bestimmungen aus Abschnitt 4.5.1.

9.6.4 Verpflichtung des Zertifikatprüfers

Es gelten die Bestimmungen aus Abschnitt 4.5.2.

9.6.5 Verpflichtung anderer Teilnehmer

Sofern weitere Teilnehmer als Dienstleister in den Zertifizierungsprozess eingebunden werden, ist die beauftragende Zertifizierungsstelle in der Verantwortung, den Dienstleister zur Einhaltung der CP zu verpflichten.

9.7 Gewährleistung

Der DFN-Verein und die innerhalb der DFN-PKI operierenden Zertifizierungsstellen übernehmen keine Gewähr dafür, dass die für die Zertifizierung benötigten Datenverarbeitungssysteme ohne Unterbrechung betriebsbereit sind und fehlerfrei arbeiten. Datenverluste in Folge technischer Störungen und die Kenntnisnahme vertraulicher Daten durch unberechtigte Eingriffe sind auch bei Beachtung der erforderlichen Sorgfalt nie völlig auszuschließen.

9.8 Haftungsbeschränkung

Der DFN-Verein und die innerhalb der DFN-PKI operierenden Zertifizierungsstellen haften wie folgt:

- **Bei vorsätzlichen oder grob fahrlässigen Pflichtverletzungen sowie im Fall der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit uneingeschränkt, soweit gesetzlich nichts anderes bestimmt ist.**
- **Bei grober Fahrlässigkeit nicht leitender Angestellter ist die Haftung für Sach- und Vermögensschäden auf den vertragstypischen und vorhersehbaren Schaden begrenzt.**
- **Bei sonstiger Fahrlässigkeit haften die Vertragsparteien für Sach- und Vermögensschäden nur bei Verletzung wesentlicher Vertragspflichten (Kardinalpflichten).**

Dabei ist die Haftung ebenfalls auf den vertragstypischen und vorhersehbaren Schaden begrenzt. Soweit die Haftung nach Satz 2 bis 4 für Sach- und Vermögensschäden auf den vertragstypischen und vorhersehbaren Schaden begrenzt ist, gilt dies auch für entgangenen Gewinn und ausgebliebene Einsparungen. Zudem ist in diesen Fällen die Haftung für entferntere Mangelfolgeschäden ausgeschlossen. Der Einwand des Mitverschuldens bleibt unberührt. Eine weitergehende Haftung ist ausgeschlossen.

9.9 Haftungsfreistellung

Für die Verwendung des dem Zertifikat zu Grunde liegenden geheimen Schlüssels haftet ausschließlich der Zertifikatnehmer. Sollten der DFN-Verein und die innerhalb der DFN-PKI operierenden Zertifizierungsstellen insoweit von einem Dritten in Anspruch genommen werden, stellt der Zertifikatnehmer den DFN-Verein und die innerhalb der DFN-PKI operierenden Zertifizierungsstellen von der Haftung frei.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Diese CP und das zugehörige CPS - in der jeweils aktuellen Fassung - treten an dem Tag in Kraft, an dem sie über den Informationsdienst (siehe Abschnitt 2.2) der PCA veröffentlicht werden.

9.10.2 Aufhebung

Dieses Dokument ist solange gültig, bis

- **es durch eine neue Version ersetzt wird oder**
- **der Betrieb der durch den DFN-Verein betriebenen Zertifizierungsstellen eingestellt wird.**

9.10.3 Konsequenzen der Aufhebung

Von einer Aufhebung der CP und des zugehörigen CPS unberührt bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Andere als die in diesem CP festgelegten Benachrichtigungen bleiben den Zertifizierungsstellen freigestellt.

9.12 Änderungen der Richtlinien

Eine Änderung der Richtlinien kann nur durch den DFN-Verein erfolgen. Einzelheiten sind in Abschnitt 1.5 des CPS festgelegt

9.13 Konfliktbeilegung

Bei Streitigkeiten im Rahmen der vorliegenden CP, an denen der DFN-Verein nicht beteiligt ist, kann der Versuch einer Streitbeilegung unter Vermittlung des DFN-Vereins unternommen werden. Ein solcher Vermittlungsversuch hat keine Auswirkung auf gesetzliche Verjährungsfristen.

9.14 Geltendes Recht

CP, CPS und der Betrieb der DFN-PKI unterliegen den Gesetzen der Bundesrepublik Deutschland.

9.15 Konformität mit dem geltenden Recht

Der DFN-Verein erhebt nicht den Anspruch, ein Zertifizierungsdienstanbieter im Sinne des deutschen Signaturgesetzes [SigG] zu sein oder qualifizierte Zertifikate auszustellen. Es werden Zertifikate ausgestellt, mit denen fortgeschrittene elektronische Signaturen gemäß dem deutschen Signaturgesetz erzeugt werden können. Diese können gegebenenfalls im Zuge der freien Beweiswürdigung vor Gericht Beweiseignung erlangen.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Alle in CP und CPS enthaltenen Regelungen gelten zwischen einer innerhalb der DFN-PKI operierenden Zertifizierungsstelle und deren Zertifikatnehmern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Übertragung der Rechte

Keine

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser CP und des zugehörigen CPS unwirksam sein oder Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.

Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung weitgehend entspricht. Im Falle von Lücken gilt dasjenige als vereinbart, was nach Sinn und Zweck dieser CP und des zugehörigen CPS vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vorn herein bedacht.

Es wird ausdrücklich vereinbart, dass sämtliche Bestimmungen dieser CP und des zugehörigen CPS, die eine Haftungsbeschränkung, den Ausschluss oder die Beschränkung von Gewährleistungen oder sonstigen Verpflichtungen oder den Ausschluss von Schadensersatz vorsehen, als eigenständige Regelungen und unabhängig von anderen Bestimmungen bestehen und als solche durchzusetzen sind.

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

Rechtliche Auseinandersetzungen, die aus dem Betrieb einer innerhalb der DFN-PKI operierenden Zertifizierungsstelle herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand sind Sitz des jeweiligen Betreibers.

9.17 Andere Regelungen

Keine

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-BASIC] Zertifizierungsrichtlinie (CP) – Sicherheitsniveau Basic, Version 1.1, DFN-Verein, 2005

[CPS-BASIC] Erklärung zum Zertifizierungsbetrieb (CPS) – Sicherheitsniveau Basic, 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