Zertifizierungsrichtlinie der

DFN-PKI

- Sicherheitsniveaus: Global, Classic und Basic -

DFN-Verein

CP der DFN-PKI

V2.1

Dezember 2006

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 Entwicklung und Erprobung neuer Anwendungen in Deutschland. Auf dieser Basis stellt der DFN-Verein seinen Anwendern Dienste zur Verfügung. Einer dieser Dienste ist die Bereitstellung einer Public Key Infrastruktur im Deutschen Forschungsnetz (DFN-PKI). Informationen zur DFN-PKI sind unter http://www.pki.dfn.de erhältlich.

1.1 Überblick

Innerhalb der DFN-PKI werden mehrere Sicherheitsniveaus unterstützt. Alle Regelungen in dieser Zertifizierungsrichtlinie (CP) gelten gleichermaßen für die Sicherheitsniveaus "Global", "Classic" und "Basic", außer in den Fällen, wo dies im Text explizit anders gekennzeichnet ist. Ein Überblick über die Sicherheitsniveaus ist in Tabelle 1 dargestellt.

Sicherheitsniveau	Identifizierung	Wurzelzertifikat	Betreiber der CA
Global	Persönlich	In Standardbrowsern verankert	DFN-Verein
Classic	Persönlich	Selbstsigniert	DFN-Verein, Anwender, Dritte
Basic	Auch schwächer als persönlich	Selbstsigniert	DFN-Verein, Anwender, Dritte

Tabelle 1: Überblick über die Sicherheitsniveaus der DFN-PKI

Dieses Dokument ist die CP der DFN-PKI für die Sicherheitsniveaus "Global", "Classic" und "Basic". Sie regelt die Abläufe innerhalb der DFN-PKI und legt dabei insbesondere die Rahmenbedingungen für die Ausstellung von Zertifikaten entsprechend der internationalen Norm X.509 [X.509] fest.

Innerhalb der gesamten DFN-PKI gibt es für die Sicherheitsniveaus "Global", "Classic" und "Basic" nur diese eine CP. Alle in dieser CP angegebenen Regelungen sind für alle Teilnehmer der DFN-PKI verbindlich und können nicht abgeschwächt werden.

Ergänzend muss es für jede Zertifizierungsstelle (CA) in der DFN-PKI eine eigene "Erklärung zum Zertifizierungsbetrieb (CPS)" geben. Jede CA regelt in ihrem CPS, wie sie die Anforderungen der CP der DFN-PKI im Detail umsetzt und in welchem Sicherheitsniveau die CA betrieben wird.

Diese CP und alle CPS in der DFN-PKI müssen die Anforderungen aus RFC 3647 [RFC3647] berücksichtigen, insbesondere zur einheitlichen Gliederung der Dokumente.

1.2 Identifikation des Dokuments

Diese CP ist folgendermaßen identifiziert:

- Titel: Zertifizierungsrichtlinie der DFN-PKI - Sicherheitsniveaus: Global, Classic und Basic -
- Version: 2.1
- Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.5.2.1

Der OID [OID] ist wie folgt zusammengesetzt:

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) dfn-verein(22177) pki(300) cp(1) x.509(1) global/classic/basic(5) major-version(2) minor-version(1)}

Dieser OID wird nicht direkt in Zertifikate aufgenommen. Stattdessen werden je nach Sicherheitsniveau die OID aus Abschnitt 7.1.6 verwendet.

1.3 Teilnehmer der Zertifizierungsinfrastruktur

1.3.1 Zertifizierungsstellen

Den CAs obliegt die Ausstellung von Zertifikaten innerhalb der DFN-PKI.

Die oberste CA (PCA) der DFN-PKI zertifiziert ausschließlich Zertifikate von unmittelbar nachgeordneten CAs entsprechend dieser CP und dem CPS der PCA.

Der Betrieb der PCA und aller CAs im Sicherheitsniveau Global erfolgt durch den DFN-Verein. CAs in den Sicherheitsniveaus Classic und Basic können auch von Anwendern selbst oder von Dritten betrieben werden.

Jedes Zertifikat ist eindeutig einem der drei Sicherheitsniveaus Global, Classic oder Basic zugeordnet. Je nach Sicherheitsniveau können die ausgestellten Zertifikate auf unterschiedliche Wurzelzertifikate zurückgeführt werden (siehe Tabelle 2).

Sicherheitsniveau	Wurzelzertifikat
Global	Der öffentliche Schlüssel der PCA ist in einem Zertifikat enthalten ("DFN-Verein PCA Global – G01"), das durch die "Deutsche Telekom Root CA 2" ausgestellt wurde.
Classic und Basic	Der öffentliche Schlüssel der PCA ist jeweils in einem selbstsignierten Wurzelzertifikat enthalten ("DFN-Verein PCA Classic – G01" bzw. "DFN-Verein PCA Basic – G01").

Tabelle 2: Sicherheitsniveau und Wurzelzertifikat

Alle innerhalb der DFN-PKI operierenden CAs unterhalb der PCA können Zertifikate für natürliche Personen und Organisationen ausstellen.

1.3.2 Registrierungsstellen

Den Registrierungsstellen (RA) obliegt die Überprüfung der Identität und Authentizität von Zertifikatnehmern.

Jeder CA innerhalb der DFN-PKI ist mindestens eine ausgezeichnete RA zugeordnet, die im CPS zu benennen ist. Nur diese RAs dürfen zur Registrierung von unmittelbar nachgeordneten CAs und RAs eingesetzt werden. Die Registrierung weiterer Zertifikatnehmer kann ebenfalls durchgeführt werden.

Alle CAs innerhalb der DFN-PKI haben die Möglichkeit, weitere RAs für die lokale Überprüfung der Identität und Authentizität der Zertifikatnehmer zu benennen. Diese RAs dürfen jedoch nicht zur Registrierung von CAs und RAs eingesetzt werden.

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

1.3.3 Zertifikatnehmer

Zertifikatnehmer sind natürliche Personen und Organisationen, an die unter Berücksichtigung der Satzung des DFN-Vereins Zertifikate vergeben werden.

1.3.4 Zertifikatprüfer

Zertifikatprüfer sind natürliche Personen und Organisationen, die unter Nutzung eines innerhalb der DFN-PKI ausgestellten Zertifikats die Identität eines Zertifikatnehmers überprüfen.

1.3.5 Weitere Teilnehmer

Weitere Teilnehmer können natürliche Personen oder Organisationen sein, die in den Zertifizierungsprozess als Dienstleister eingebunden sind. Bei Dienstleistern, die im Namen und Auftrag eines DFN-Anwenders tätig werden, liegt die Verantwortung für die Einhaltung von CP und CPS bei dem beauftragenden DFN-Anwender.

1.4 Zertifikatnutzung

1.4.1 Geeignete Zertifikatnutzung

Die im Rahmen der DFN-PKI ausgestellten Zertifikate können u.a. für Authentifizierung, elektronische Signatur und Verschlüsselung verwendet werden. Zertifikatnehmer sind selbst für die Nutzung in den Anwendungsprogrammen zuständig, sowie für die Prüfung, ob die damit möglichen Anwendungen den Sicherheitsanforderungen geeignet Rechnung tragen.

1.4.2 Untersagte Zertifikatnutzung

Grundsätzlich ist keine Zertifikatnutzung untersagt, jedoch ist die Ausstellung von Zertifikaten und Sperrlisten ausschließlich CAs vorbehalten.

1.5 Verwaltung des Dokuments

1.5.1 Organisation

Die Verwaltung dieses Dokuments erfolgt durch den DFN-Verein. Für Kontaktinformationen siehe Abschnitt 1.5.2.

1.5.2 Kontaktperson

Die Kontaktperson für dieses Dokument ist:

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

1.5.3 Verantwortliche Person für Prüfung der CPS

Die in Abschnitt 1.5.2 genannte Person ist verantwortlich für die Prüfung aller CPS in der DFN-PKI.

1.5.4 Genehmigungsverfahren für CPS

Die Genehmigung von CPS erfolgt durch den DFN-Verein bzw. durch einen von ihm beauftragten Dienstleister.

1.6 Definitionen und Abkürzungen

Siehe Kapitel 11.

2 Veröffentlichungen und Informationsdienste

2.1 Informationsdienste

Jede CA innerhalb der DFN-PKI muss die in Abschnitt 2.2 genannten Informationen gemäß Abschnitt 2.3 und Abschnitt 2.4 vorhalten.

2.2 Veröffentlichung von Informationen

Jede CA innerhalb der DFN-PKI muss folgende aktuelle Informationen veröffentlichen und die Adressen der entsprechenden Informationsdienste in ihrem CPS angeben:

- CP der DFN-PKI

- Sicherheitsniveau der CA (Global, Classic oder Basic)
- Zertifikat der zugehörigen PCA und dessen Fingerabdruck
- Wurzelzertifikat und dessen Fingerabdruck (nur im Sicherheitsniveau Global)
- CPS der CA
- Zertifikat der CA und dessen Fingerabdruck
- Liste der RAs, die zur CA gehören
- Verweis auf einen Verzeichnisdienst für die ausgestellten Zertifikate, sofern ein solcher betrieben wird
- Verweis auf die CRL der CA und der PCA
- Kontaktinformationen, unter denen eine Sperrung beantragt werden kann

Darüber hinaus sollten den Zertifikatnehmern Informationen über die DFN-PKI, zur Überprüfung der Gültigkeit von Zertifikaten, über die korrekte Anwendung von Kryptographie und über die Verwendung von Zertifikaten zur Verfügung gestellt werden.

2.3 Aktualisierung von Informationen

Für die Aktualisierung der in Abschnitt 2.2 genanten Informationen gelten folgende Fristen:

- Zertifikate: spätestens drei Werktage nach der Ausstellung
- CP und CPS: spätestens eine Woche nach Erstellung einer neuen Version
- Liste der RAs: spätestens drei Werktage nach einer Veränderung
- CRLs: Siehe Abschnitt 4.9.7.

2.4 Zugriff auf Informationsdienste

Der lesende Zugriff auf alle in Abschnitt 2.2 aufgeführten Informationen muss ohne Zugriffskontrolle möglich sein. Schreibender Zugriff auf diese Informationen darf nur berechtigten Personen gewährt werden. Die Informationsdienste sollen ohne zeitliche Einschränkungen zugänglich sein.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensform

In der DFN-PKI wird eine einheitliche Namenshierarchie verwendet. Alle innerhalb der DFN-PKI ausgestellten Zertifikate beinhalten eindeutige Namen (DN) gemäß der Normenserie X.500. Ein DN enthält eine Folge von eindeutig kennzeichnenden Attributen, durch die jeder Zertifikatnehmer eindeutig referenziert wird. Abweichungen sind mit dem DFN-Verein abzustimmen und müssen im CPS erläutert werden.

Ein DN entspricht grundsätzlich folgendem Schema, dabei sind optionale Attribute in eckige Klammern gesetzt, Attribute in spitzen Klammern müssen durch die jeweiligen Werte ersetzt werden. Die Reihenfolge der Attribute muss eingehalten werden.

C=DE,

[ST=<Bundesland>,]

[L=<Ort>,]

O=<Organisation>,

[OU=<Organisationseinheit>,]

[CN=<Eindeutiger Name>,]

[emailAddress=<E-Mail Adresse>]

Das Attribut "O=" enthält den Namen der Organisation, welcher der Zertifikatnehmer angehört.

Als einziges Attribut kann "OU=" mehrfach angegeben werden.

Die Verwendung des Attributs "CN=" ist bei natürlichen Personen zwingend erforderlich, ansonsten, z.B. bei Datenverarbeitungssystemen, sollte es aus Interoperabilitätsgründen verwendet werden.

Obwohl die Angabe von E-Mail Adressen im DN möglich ist, sollten diese bevorzugt in der Zertifikaterweiterung "subjectAlternativeName" aufgenommen werden.

Jede CA vereinbart mit ihrer übergeordneten CA einen eindeutigen Namensraum. Eine CA darf bei der Ausstellung von Zertifikaten nur DNs verwenden, die in ihrem vereinbarten Namensraum liegen. Die Verantwortung für die Eindeutigkeit der Namen obliegt der ausstellenden CA.

Jede CA muss ihren Namensraum in ihrem CPS veröffentlichen. Für die PCA gibt es keine Beschränkung des Namensraums.

3.1.2 Aussagekräftigkeit von Namen

Der DN muss den Zertifikatnehmer eindeutig identifizieren. Bei der Namensvergabe gelten die folgenden Regelungen:

- Zertifikate für natürliche Personen dürfen nur auf einen zulässigen Namen des Zertifikatnehmers ausgestellt werden. Namenszusätze dürfen nur verwendet werden, wenn diese in einem amtlichen Ausweispapiers mit Lichtbild enthalten sind, z.B. "CN=Manuela Musterfrau, Dr.".
- Zertifikate für Personengruppen müssen mit dem Kennzeichen "GRP:" beginnen, z.B. "CN=GRP:Poststelle". Bei CAs und RAs kann darauf verzichtet werden, wenn die Funktion aus dem CN erkennbar ist. Bei der Vergabe von Namen für Personengruppen muss eine Verwechslung mit existierenden Namen, z.B. mit natürlichen Personen oder Organisationen, 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 muss für den Namen der voll qualifizierte Domainname verwendet werden, z.B. "CN=pki.pca.dfn.de". Insbesondere sind sogenannte "Wildcard Zertifikate", z.B. "CN=*.pca.dfn.de" nicht zulässig.
- Bei der Vergabe von Namen für Pseudonyme muss eine Verwechslung mit existierenden Namen, z.B. mit natürlichen Personen oder Organisationen, 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. Der CN eines Pseudonyms muss mit dem Kennzeichen "PN:" beginnen, z.B. "CN=PN:Deckname".
- Der CN für externe Zertifikatnehmer, die keinem DFN-Anwender angehören und die nicht im Namen und Auftrag eines DFN-Anwenders handeln, muss mit dem Kennzeichen "EXT:" beginnen, z.B. "CN=EXT:Max Mustermann".

3.1.3 Anonymität und Pseudonymität

Für natürliche Personen kann anstelle des Namens im Zertifikat ein Pseudonym aufgeführt werden. Dieses muss im CN eindeutig kenntlich gemacht werden (siehe Abschnitt 3.1.2).

Die PCA bietet die Ausstellung von pseudonymen Zertifikaten nicht an. Falls eine CA Pseudonyme erlaubt, müssen Details zu den zulässigen Pseudonymen im entsprechenden CPS geregelt werden.

Anonyme Zertifikate dürfen nicht ausgestellt werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Ausschließlich die folgenden Zeichen dürfen in Namen verwendet werden:

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

Für die Ersetzung deutscher Sonderzeichen gelten folgende Substitutionsregeln:

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

Sonderzeichen mit Akzenten verlieren diese. 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.

3.1.5 Eindeutigkeit von Namen

Vor der Zertifizierung muss die Korrektheit und Eindeutigkeit des angegebenen Namens von der zuständigen CA überprüft werden. Der DN eines Zertifikatnehmers muss eindeutig sein und darf nicht an unterschiedliche Zertifikatnehmer vergeben werden.

Bei Namensgleichheit gilt grundsätzlich das Prinzip: "Wer zuerst kommt, wird zuerst bedient". In Streitfällen entscheidet die zuständige CA.

Darüber hinaus muss jedem Zertifikat durch die ausstellende CA eine eindeutige Seriennummer zugeordnet werden, die eine eindeutige und unveränderliche Zuordnung zum Zertifikatnehmer ermöglicht.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Sofern sich der DN eines Zertifikats auf eine natürliche Person bezieht, ist eine Anerkennung von Warenzeichen nicht relevant. In allen anderen Fällen liegt es in der alleinigen Verantwortung des Zertifikatnehmers, dass die Namenswahl keine Warenzeichen, Markenrechte usw. verletzt. Die CAs sind nicht verpflichtet, solche Rechte zu überprüfen. Falls eine CA über eine Verletzung solcher Rechte informiert wird, muss sie das Zertifikat sperren.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Erfolgt die Schlüsselgenerierung nicht bei einer CA, muss der Zertifikatnehmer bei der Zertifikatbeantragung versichern, dass er im Besitz des privaten Schlüssels ist.

Dies geschieht, indem der öffentliche Schlüssel vom Zertifikatnehmer in einem mit dem zugehörigen privaten Schlüssel elektronisch signierten Zertifikatantrag (CSR) an die RA übermittelt wird. Die RA muss die Gültigkeit der Signatur überprüfen. Zusätzlich muss die Authentizität des CSR, z.B. durch handschriftliche Unterschrift des Zertifikatnehmers, bestätigt werden.

3.2.2 Authentifizierung einer Organisation

Zertifikate für Organisationen werden immer durch natürliche Personen beantragt, deren Authentifizierung gemäß Abschnitt 3.2.3 erfolgen muss. Zusätzlich erfolgt die Authentifizierung einer Organisation im Rahmen der Registrierung durch die Vorlage aussagekräftiger Unterlagen.

3.2.3 Authentifizierung einer natürlichen Person

Für die Authentifizierung der Identität einer natürlichen Person gibt es die folgenden Verfahren.

a) Der Zertifikatnehmer erscheint persönlich bei einer zuständigen RA. Ein Mitarbeiter der RA führt die Identitätsprüfung anhand eines amtlichen Ausweispapiers mit Lichtbild (Personalausweis oder Reisepass) durch.
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) durchführt und entsprechend dokumentiert. Die genutzte Dienstleistung muss entweder über eine Konformitätsbestätigung für die Umsetzung von Sicherheitskonzepten durch eine von der Bundesnetzagentur [BNA] anerkannten Prüf- und Bestätigungsstelle verfügen oder ein konformes Verhalten muss durch vertragliche Regelungen verpflichtend gemacht werden.

c) Die Authentifizierung einer natürlichen Person kann 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.

Die je Sicherheitsniveau zulässigen Verfahren sind in Tabelle 3 dargestellt. Insbesondere ist zu beachten, dass Verfahren c) ausschließlich für das Sicherheitsniveau Basic zulässig ist. Handelt es sich bei dem Zertifikatnehmer um eine CA oder RA, ist eine Überprüfung der Identität und Authentizität immer gemäß Verfahren a) notwendig.

Sicherheitsniveau	Zertifikattyp		Verfahren		
	RA/CA	andere	a)	b)	c)
Global	X		zulässig	---------	---------
Global		X	zulässig	zulässig	---------
Classic	X		zulässig	---------	---------
Classic		X	zulässig	zulässig	---------
Basic	X		zulässig	---------	---------
Basic		X	zulässig	zulässig	zulässig

Tabelle 3: Zulässige Verfahren zur Authentifizierung einer natürlichen Person

Bei allen Verfahren müssen folgende Informationen vorliegen und überprüft werden:

- Name, Vorname(n) und Namenszusätze soweit im Ausweispapier vermerkt
- E-Mail Adresse
- Art und letzte fünf Zeichen der Nummer des Ausweispapiers
- Name und Anschrift der zugehörigen Organisation
- Nachweis der Zugehörigkeit zur angegebenen Organisation

3.2.4 Nicht überprüfte Informationen

Außer den Angaben in Abschnitt 3.2.2 und Abschnitt 3.2.3 werden keine weiteren Informationen überprüft.

3.2.5 Unterschriftenvollmacht

Die Bevollmächtigung einer handlungsberechtigten Person (HP) durch die beantragende Organisation muss in schriftlicher oder geeigneter elektronisch signierter Form durch eine zur Unterschrift bevollmächtigte Person erfolgen. Bevollmächtigte HP können weitere Bevollmächtigungen für die Organisation erteilen.

Jede HP muss nach Abschnitt 3.2.3 a) authentifiziert werden.

3.2.6 Cross-Zertifizierung

Die Möglichkeit der Cross-Zertifizierung besteht ausschließlich für die PCA.

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

3.3.1 Routinemäßige Zertifikaterneuerung

Verfügt die beantragende Person über ein gültiges Zertifikat, so kann die Identifizierung und Authentifizierung zur Zertifikaterneuerung auch unter Verwendung dieses Zertifikats durchgeführt werden. Die Authentifizierung von Zertifikatanträgen mittels handschriftlicher Unterschrift des Zertifikatnehmers ist ebenfalls zulässig.

3.3.2 Zertifikaterneuerung nach einer Sperrung

Nach dem Sperren eines Zertifikats kann eine Authentifizierung nicht mehr mit dem gesperrten Zertifikat durchgeführt werden.

3.4 Identifizierung und Authentifizierung bei einer Sperrung

Die Authentifizierung einer Sperrung kann auf die folgenden Arten erfolgen:

- Übermittlung einer vorher vereinbarten Authentisierungsinformation (schriftlich, per Telefon, oder elektronisch)
- Übergabe eines Sperrantrags mit einer handschriftlicher Unterschrift
- Übergabe eines Sperrantrags mit einer geeigneten elektronischen Signatur, die den Zertifikatnehmer authentifiziert

4 Ablauforganisation

4.1 Zertifikatantrag

4.1.1 Wer kann ein Zertifikat beantragen

In der DFN-PKI können Zertifikatnehmer gemäß Abschnitt 1.3.3 Zertifikate beantragen. CAs können den Kreis der berechtigten Zertifikatnehmer in ihrem CPS weiter eingrenzen.

4.1.2 Registrierungsprozess

Um ein Zertifikat zu erhalten, muss ein Antrag bei der zuständigen Registrierungsstelle eingereicht werden.

Bei der Registrierungsstelle müssen die folgenden Arbeitsschritte durchlaufen und dokumentiert werden:

- Prüfung des Zertifikatantrags hinsichtlich Vollständigkeit und Korrektheit
- Prüfung der Eindeutigkeit des gewünschten DN
- Prüfung des Vorliegens beziehungsweise Durchführung einer Authentifizierung der Identität nach Abschnitt 3.2.3
- Gegebenenfalls Überprüfung der Authentifizierung einer Organisation nach Abschnitt 3.2.2
- Überprüfung des Besitzes des privaten Schlüssels nach Abschnitt 3.2.1
- sichere Archivierung der beim Zertifizierungsprozess anfallenden Unterlagen, Papierunterlagen müssen in einem verschlossenem Schrank aufbewahrt werden

Die Übermittlung der für die Zertifizierung notwendigen Informationen an die zuständige CA erfolgt entweder verschlüsselt und signiert auf elektronischem Weg unter Verwendung des Zertifikats der zuständigen RA oder auf postalischem Weg.

4.2 Bearbeitung von Zertifikatanträgen

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die Identifizierung und Authentifizierung von Zertifikatnehmern wird gemäß Abschnitt 3.2 durchgeführt.

4.2.2 Annahme oder Abweisung von Zertifikatanträgen

Ein Zertifikatantrag wird von der zuständigen RA akzeptiert, wenn alle Arbeitsschritte gemäß Abschnitt 4.1.2 erfolgreich durchlaufen wurden. Andernfalls wird der Zertifikatantrag abgewiesen und dies dem Antragsteller unter Angabe von Gründen mitgeteilt.

4.2.3 Bearbeitungsdauer

Die Bearbeitungsdauer eines Zertifikatantrags beträgt grundsätzlich maximal eine Woche.

4.3 Zertifikatausstellung

4.3.1 Aktionen der Zertifizierungsstelle während der Zertifikatausstellung

Die formalen Voraussetzungen für die Ausstellung eines Zertifikats werden durch die CA in angemessener Weise überprüft. Insbesondere überprüft die CA die Berechtigung der RA, ein Zertifikat für den im DN angegebenen Namen zu genehmigen sowie die Gültigkeit der Signatur der RA.

4.3.2 Benachrichtigung des Zertifikatnehmers nach der Zertifikatausstellung

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

4.4 Zertifikatakzeptanz

Der Zertifikatnehmer ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der ausstellenden CA 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 von 14 Tagen nach Erhalt kein Widerspruch erfolgt. Durch Annahme des Zertifikats versichert der Zertifikatnehmer, dass sämtliche Angaben und Erklärungen in Bezug auf die im Zertifikat enthaltenden Informationen der Wahrheit entsprechen.

4.4.2 Veröffentlichung des Zertifikats

Wenn der Veröffentlichung eines Zertifikats nicht widersprochen wurde, wird dieses von einer CA über einen Informationsdienst (siehe Kapitel 2) veröffentlicht.

4.4.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist nicht erforderlich.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatnehmer

Der Zertifikatnehmer muss Sorge tragen, dass sein privater Schlüssel angemessen geschützt ist und das Zertifikat in Übereinstimmung mit diesem CP eingesetzt wird.

Das Zertifikat ist unverzüglich zu sperren, wenn die Angaben des Zertifikats nicht mehr korrekt sind oder wenn der private Schlüssel abhanden gekommen, gestohlen oder möglicherweise kompromittiert wurde.

Bietet eine CA keine Möglichkeit der Schlüsselhinterlegung an oder wird eine optionale Schlüsselhinterlegungsmöglichkeit bei der CA vom Zertifikatnehmer nicht in Anspruch genommen, so ist der Zertifikatnehmer selbst dafür zuständig, private Schlüssel so zu sichern, dass er ggf. verschlüsselte Daten wieder entschlüsseln kann.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Zertifikatprüfer

Zertifikatprüfer sollten vor der Nutzung eines Zertifikats dessen Gültigkeit überprüfen und das Zertifikat ausschließlich in Übereinstimmung mit dieser CP einsetzen.

4.6 Zertifikaterneuerung ohne Schlüsselwechsel

Bei einer Zertifikaterneuerung ohne Schlüsselwechsel wird einem Zertifikatnehmer durch die zuständige CA ein neues Zertifikat unter Beibehaltung des alten Schlüsselpaars ausgestellt, sofern das Schlüsselpaar den kryptographischen Mindestanforderungen der aktuellen

CP genügt, die im Zertifikat enthaltenen Informationen unverändert bleiben und kein Verdacht auf Kompromittierung des privaten Schlüssels vorliegt.

4.6.1 Gründe für eine Zertifikaterneuerung

Eine Zertifikaterneuerung kann beantragt werden, wenn die Gültigkeit eines Zertifikats abläuft.

4.6.2 Wer kann eine Zertifikaterneuerung beantragen?

Eine Zertifikaterneuerung wird grundsätzlich durch den Zertifikatnehmer beantragt. Es obliegt der zuständigen CA, ob sie eine Zertifikaterneuerung aktiv unterstützt.

4.6.3 Ablauf der Zertifikaterneuerung

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

4.6.4 Benachrichtigung des Zertifikatnehmers

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 mit Schlüsselwechsel

Bei einer Zertifikaterneuerung mit Schlüsselwechsel wird einem Zertifikatnehmer, der bereits ein Zertifikat besitzt, durch die zuständige CA ein neues Zertifikat für ein neues Schlüsselpaar ausgestellt, sofern die im Zertifikat enthaltenen Informationen unverändert bleiben. Es wird analog zu Abschnitt 4.6 vorgegangen.

4.8 Zertifikatmodifizierung

Eine Zertifikatsmodifizierung kann vorgenommen werden, wenn sich die im Zertifikat enthaltenen Informationen (z.B. der Verwendungszweck) verändern. Dabei kommen sinngemäß die Regelungen aus Abschnitt 4.6 zur Anwendung. Sofern sich die Identität des Zertifikatnehmers geändert hat, ist wie bei einem Neuantrag zu verfahren. Das alte Zertifikat muss nach Ausstellung des neuen Zertifikats gesperrt werden.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für eine Sperrung

Ein Zertifikat muss gesperrt werden, wenn mindestens einer der folgenden Gründe vorliegt:

- Das Zertifikat enthält Angaben, die nicht gültig sind.
- Der private Schlüssel des Zertifikatnehmers wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Der Zertifikatnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen (siehe Abschnitt 1.3.3).
- Der Zertifikatnehmer hält die CP nicht ein.
- Der Zertifikatnehmer verlangt die Sperrung des Zertifikats.
- Die zuständige CA bzw. eine RA hält die CP oder das CPS nicht ein.
- Die CA stellt den Zertifizierungsbetrieb ein.

4.9.2 Wer kann eine Sperrung beantragen?

Sperrungen können vom Zertifikatnehmer oder von der zuständigen RA beantragt werden. Dritte können eine Sperrung beantragen, wenn sie Beweise vorlegen, dass einer der unter Abschnitt 4.9.1 genannten Gründe für eine Sperrung vorliegt.

4.9.3 Ablauf einer Sperrung

Verlangen Zertifikatnehmer eine Sperrung, so müssen sie sich gegenüber der zuständigen RA authentifizieren. Die möglichen Verfahren sind in Abschnitt 3.4 dargestellt.

Hat die RA erfolgreich den Zertifikatnehmer authentifiziert oder selber einen Sperrantrag gestellt, so genehmigt sie diesen und leitet ihn an die CA weiter.

Die CA führt die Sperrung durch, nachdem sie die Berechtigung der RA für die Sperrung des Zertifikats und die Signatur der RA geprüft hat.

4.9.4 Fristen für Stellung eines Sperrantrags

Wenn Gründe (siehe Abschnitt 4.9.1) für eine Sperrung vorliegen, muss unverzüglich ein Sperrantrag gestellt werden.

4.9.5 Fristen für die Sperrung

Eine CA muss eine Zertifikatsperrung unverzüglich vornehmen, wenn die Voraussetzungen dafür gegeben sind (siehe Abschnitt 4.9.3).

4.9.6 Anforderungen zur Kontrolle der CRL durch den Zertifikatprüfer

Siehe Abschnitt 4.5.2.

4.9.7 Veröffentlichungsfrequenz für CRLs

CRLs müssen mindestens einmal pro Monat erstellt und veröffentlicht werden. Wird ein Zertifikat gesperrt, muss umgehend eine neue CRL erstellt und veröffentlicht werden.

4.9.8 Maximale Latenzzeit für CRLs

Nach Erzeugung neuer CRLs müssen diese umgehend veröffentlicht werden.

4.9.9 Verfügbarkeit von Online Sperr- und Statusüberprüfungsverfahren

Wenn ein Online Sperr- und Statusüberprüfungsverfahren (z.B. OCSP) angeboten wird, sind die Details dazu im CPS zu vermerken.

4.9.10 Anforderungen an Online Sperr- und Statusüberprüfungsverfahren

Es gelten die Anforderungen zum Schutz des privaten Schlüssels gemäß Abschnitt 6.2.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrungen

Keine Angaben.

4.9.12 Kompromittierung von privaten Schlüsseln

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

4.9.13 Gründe für eine Suspendierung

Eine Suspendierung (zeitliche Aussetzung) von Zertifikaten ist nicht erlaubt. Einmal gesperrte Zertifikate können nicht erneuert oder verlängert werden.

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

Die Pflicht jeder CA zur Bereitstellung einer CRL ist in Kapitel 2 geregelt.

Werden weitere Dienste zur Statusabfrage von Zertifikaten (z.B. OCSP) von einer CA angeboten, sind die Verfahrensmerkmale, die Verfügbarkeit des Dienstes und die optionalen Merkmale im zugehörigen CPS aufzuführen.

4.11 Beendigung der Zertifikatnutzung durch den Zertifikatnehmer

Eine Beendigung der Zertifikatnutzung erfolgt durch Zertifikatnehmer entweder durch eine Sperrung oder indem nach Ablauf der Gültigkeit kein neues Zertifikat beantragt wird.

4.12 Schlüsselhinterlegung und -wiederherstellung

4.12.1 Richtlinien u. Praktiken zur Schlüsselhinterlegung und –wiederherstellung

Wenn die Dienstleistungen Schlüsselhinterlegung und -wiederherstellung von einer CA angeboten werden, so sind die Richtlinien und Praktiken im zugehörigen CPS ausführlich zu beschreiben.

Die PCA bietet keine Schlüsselhinterlegung und -wiederherstellung für Zertifikatnehmer an.

4.12.2 Richtlinien und Praktiken zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung

Entfällt.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI. Diese Sicherheitsmaßnahmen müssen von jeder CA in ihrem CPS in ihren wesentlichen Grundzügen beschrieben werden. Detaillierte Informationen sollten in einem Sicherheitskonzept festgeschrieben werden. Dieses muss nicht veröffentlicht werden, aber im Rahmen der Konformitätsprüfung (siehe Kapitel 8) zur Verfügung stehen.

Sofern dabei einzelne Sicherheitsmaßnahmen nicht spezifiziert werden, sind diese grundsätzlich an die Maßnahmenkataloge des IT-Grundschutzhandbuchs [IT-GSHB] anzulehnen.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Jede CA muss in ihrem CPS die infrastrukturellen Sicherheitsmaßnahmen beschreiben, dies kann exemplarisch dem CPS der PCA entnommen werden.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitsrelevante Rollen

In Tabelle 4 sind die sicherheitsrelevanten Rollen definiert, die im Rahmen des Zertifizierungsprozesses erforderlich sind. Um einen ordnungsgemäßen und revisionssicheren Betrieb einer CA zu gewährleisten, muss eine entsprechende Aufgabenverteilung und Funktionstrennung vorgenommen werden. Es ist möglich, eine Rolle auf mehrere Mitarbeiter zu verteilen. Ebenso kann ein Mitarbeiter in mehr als einer Rolle auftreten, dabei sind die Rollenunverträglichkeiten aus Abschnitt 5.2.4 zu beachten.

Erweiterungen am Rollenmodell sind möglich, müssen aber im CPS beschrieben werden.

Rolle	Aufgabe der Rolle	Kürzel
Teilnehmerservice	Entgegennahme von Zertifikat- und Sperranträgen. Authentifizierung der Identität und Prüfung der Autorisierung der Zertifikatnehmer. Verifikation der Dokumente. Beratung der Zertifikatnehmer.	TS
Registrator	Prüfung von Zertifikat- und Sperranträgen hinsichtlich Vollständigkeit und Korrektheit. Archivierung von Dokumenten. Freigabe, Übermittlung von Zertifikat- und Sperranträgen an die zuständige CA.	RG
CA-Mitarbeiter	Verantwortlich für Anwendung und Lagerung von elektronischen Datenträgern, auf denen die privaten Schlüssel der CA gespeichert sind. Kenntnis der ersten Hälfte der PINs (Passwörter) der privaten Schlüssel der CA.	CAO1
PIN-Geber	Kenntnis der zweiten Hälfte der PINs der privaten Schlüssel der CA.	CAO2
System- und Netzwerkadministrator	Installation, Konfiguration, Administration und Wartung der IT- und Kommunikationssysteme. Kontrolle über die eingesetzte Hard- und Software, jedoch kein Zugriff auf und keine Kenntnis von kryptographischen Schlüsseln und deren PINs für den Zertifizierungsprozess. Ausschließliche Kenntnis der Boot- und Administrator-Passwörter der Systeme.	SA
Systemoperator	Betreuung der Datensicherung und –wiederherstellung der erforderlichen Server und der CA-Anwendungssoftware.	SO
Revision	Durchführung der betriebsinternen Audits und der Audits von Sub-CAs, Überwachung und Einhaltung der Datenschutzbestimmungen.	R
Sicherheitsbeauftragter	Definition und Überprüfung der Einhaltung der Sicherheitsbestimmungen, insbesondere CPS und Sicherheitskonzept. Zuordnung von Personen zu Rollen und zu Berechtigungen. Ansprechpartner für sicherheitsrelevante Fragen.	ISO

Tabelle 4: Rollen

5.2.2 Erforderliche Anzahl von Personen je Tätigkeit

In Tabelle 5 sind die Tätigkeiten beschrieben, bei denen das Vier-Augen-Prinzip - realisiert durch jeweils einen Vertreter der angegebenen Rollen - eingehalten werden muss. Alle anderen Tätigkeiten können von einer Person durchgeführt werden.

Tätigkeit	Rollen
Freigabe und Übermittlung von Zertifikat- und Sperranträgen für CA-Zertifikate	RG & TS
Erzeugung von Schlüsselpaaren für CA-Zertifikate	CAO1 & CAO2
Starten von Prozessen zur Ausstellung von Zertifikaten und Sperrlisten	CAO1 & CAO2
Austausch von Hard- und Softwarekomponenten für die Zertifizierung	SA & CAO1

Tabelle 5: Tätigkeiten, die das Vier-Augen-Prinzip erfordern

5.2.3 Identifizierung und Authentifizierung der Rollen

Die Identifizierung und Authentifizierung der Rollen muss auf Grundlage des in Abschnitt 5.2.1 und Abschnitt 5.2.2 beschriebenen Rollenmodells erfolgen. Der technische Zugang zu den IT-Systemen wird durch Nutzerkennung und Passwort oder ein stärkeres Verfahren realisiert, eine Regelung zum Passwortgebrauch ist vorzuhalten. Der physikalische Zugang

zu den IT-Systemen muss durch Zutrittskontrollmaßnahmen reglementiert werden. Der Zugang zu Bankschließfächern muss neben dem Besitz des zugehörigen Schlüssels mit einer persönlichen Identifizierung und Authentifizierung verbunden sein.

5.2.4 Trennung von Rollen

In Tabelle 6 ist aufgeführt, welche Rollen miteinander unverträglich sind.

Rolle	Unverträglich mit							
	TS	RG	CAO1	CAO2	SA	SO	R	ISO
TS – Teilnehmerservice					X	X	X	X
RG – Registrator					X	X	X	X
CAO1 - CA Mitarbeiter				X	X	X	X	X
CAO2 - PIN Geber			X				X	X
SA – Systemadministrator	X	X	X				X	X
SO – Systemoperator	X	X	X				X	X
R - Revision	X	X	X	X	X	X		
ISO – Sicherheitsbeauftragter	X	X	X	X	X	X		

Tabelle 6: Unverträglichkeit von Rollen

Jede CA muss in ihrem CPS darstellen, wie die Aufteilung der Rollen auf Personengruppen vorgenommen wird. Dabei dürfen keiner Person miteinander unverträgliche Rollen zugewiesen werden.

5.3 Personelle Sicherheitsmaßnahmen

Jede CA muss in ihrem CPS die personellen Sicherheitsmaßnahmen beschreiben. Dies kann exemplarisch dem CPS der PCA entnommen werden.

5.4 Sicherheitsüberwachung

Jede CA muss in ihrem CPS die Maßnahmen zur Sicherheitsüberwachung beschreiben. Dies kann exemplarisch dem CPS der PCA entnommen werden.

5.5 Archivierung

Jede CA muss in ihrem CPS die Maßnahmen zur Archivierung beschreiben. Dies kann exemplarisch dem CPS der PCA entnommen werden.

5.6 Schlüsselwechsel

Die Gültigkeitsdauer von Schlüsseln ist in Abschnitt 6.3.2 festgelegt. Falls ein Schlüssel der CA kompromittiert wurde, gelten die in Abschnitt 5.7 aufgeführten Regelungen. Nach Erzeugung eines neuen CA-Schlüssels muss dieser gemäß Kapitel 2 veröffentlicht werden.

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 einer CA müssen schriftlich dokumentiert und an alle Mitarbeiter ausgehändigt werden. Die Grundzüge der Prozeduren sind in den folgenden Unterkapiteln aufgeführt.

5.7.2 Prozeduren bei IT-Systemen

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

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

5.7.3 Kompromittierung von privaten Schlüsseln

Wurde ein privater Schlüssel eines Zertifikatnehmers kompromittiert, so muss das dazugehörige Zertifikat gesperrt werden (siehe Abschnitt 4.9.1).

Wurde der private Schlüssel einer CA kompromittiert, so müssen das Zertifikat der CA und alle damit ausgestellten Zertifikate gesperrt werden. Außerdem müssen alle betroffenen Zertifikatnehmer informiert werden.

5.7.4 Betrieb nach einer Katastrophe

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

5.8 Einstellung des Betriebs

Stellt eine CA ihren Betrieb ein, müssen folgende Maßnahmen ergriffen werden:

- Information aller Zertifikatnehmer, betroffenen RAs und der Kontaktperson aus Abschnitt 1.5.2 mindestens drei Monate vor Einstellung des Betriebs
- Sperrung aller von der CA ausgestellten Zertifikate
- sichere Zerstörung der privaten Schlüssel der CA

Der Betreiber der CA muss den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen Sperrliste für den zugesicherten Aufbewahrungszeitraum (siehe Abschnitt 5.5) sicherstellen.

6 Technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter technischer Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI. Diese Sicherheitsmaßnahmen müssen von jeder CA in ihrem CPS in ihren wesentlichen Grundzügen beschrieben werden. Detaillierte Informationen sollten in einem Sicherheitskonzept festgeschrieben werden. Dieses muss nicht veröffentlicht werden, aber im Rahmen der Konformitätsprüfung (siehe Kapitel 8) zur Verfügung stehen.

Sofern dabei einzelne Sicherheitsmaßnahmen nicht spezifiziert werden, sind diese grundsätzlich an die Maßnahmenkataloge des IT-Grundschutzhandbuchs [IT-GSHB] anzulehnen.

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Die Schüsselpaare aller CAs müssen entweder auf einem IT-System ohne Netzwerkanschluss erzeugt werden, oder in einem Hardware Sicherheitsmodul (HSM), das den Anforderungen aus Abschnitt 6.2.1 genügt.

Für RAs kann eine Schlüsselerzeugung bei der RA oder der zugehörigen CA durchgeführt werden. Wird der Schlüssel bei der CA erzeugt, ist das Verfahren im CPS darzulegen.

Für Zertifikatnehmer kann die Schlüsselerzeugung durch diesen selbst oder bei der zugehörigen RA bzw. CA durchgeführt werden. Wird der Schlüssel bei der RA oder CA erzeugt, ist das Verfahren im CPS darzulegen.

6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatnehmer

Ist eine Übermittlung des privaten Schlüssels an einen Zertifikatnehmer oder eine RA notwendig, so ist der private Schlüssel während der Übermittlung ausreichend zu sichern und das Verfahren im CPS darzulegen.

6.1.3 Übermittlung des öffentlichen Schlüssels an den Zertifikataussteller

Der CSR des Zertifikatnehmers wird per E-Mail, HTTPS oder auf einem Datenträger an die CA übermittelt. Die Zugehörigkeit des CSR zu einem bestimmten Zertifikatantrag wird durch Unterschrift oder elektronische Signatur bestätigt.

6.1.4 Übermittlung des öffentlichen CA-Schlüssels

Alle Teilnehmer der DFN-PKI können den öffentlichen Schlüssel jeder CA über einen Informationsdienst gemäß Kapitel 2 abrufen.

6.1.5 Schlüssellängen

Im Sicherheitsniveau Global müssen bei Einsatz des RSA-Algorithmus alle verwendeten Schlüssel eine Mindestlänge von 2048 Bit haben.

In den Sicherheitsniveaus Classic und Basic muss bei Einsatz des RSA-Algorithmus die Schlüssellänge bei CAs mindestens 2048 Bit betragen, bei allen anderen Schlüsseln mindestens 1024 Bit. Zur Gewährleistung eines langfristigen Sicherheitsniveaus wird jedoch die Verwendung von mindestens 2048 Bit dringend empfohlen.

Sicherheitsniveau	RSA-Schlüssellänge für CAs	RSA-Schlüssellänge Sonstige
Global	2048 Bit	2048 Bit
Classic, Basic	2048 Bit	1024 Bit, 2048 Bit empfohlen

Tabelle 7: Überblick über die Schlüssellängen in der DFN-PKI

Darüber hinaus sind grundsätzlich alle kryptographischen Algorithmen entsprechend der aktuellen "Übersicht über geeignete Algorithmen" der Bundesnetzagentur [BNA] zulässig, wenn ihre Sicherheit mindestens äquivalent zu RSA mit 2048 Bit ist. Bei Einsatz anderer Algorithmen sind diese im CPS zu beschreiben.

6.1.6 Parameter der öffentlichen Schlüssel und Qualitätssicherung

Entfällt.

6.1.7 Verwendungszweck der Schlüssel und Beschränkungen

Entfällt.

6.2 Schutz des privaten Schlüssels

Erfolgt die Anwendung des privaten Schlüssels der CA 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

HSM, die gemäß Abschnitt 6.2 eingesetzt werden, müssen einem der folgenden bzw. dazu äquivalenten Standard genügen:

- FIPS 140-1 Level 3
- CC EAL4
- ITSEC E3 der Stärke "hoch"

6.2.2 Kontrolle des privaten Schlüssels durch mehrere Personen

Der Zugriff auf den privaten Schlüssel einer CA muss gemäß Abschnitt 6.2.8 immer im 4-Augen-Prinzip durch die Rollen CAO1 und CAO2 gemeinsam stattfinden.

6.2.3 Hinterlegung ("Key Escrow") privater Schlüssel

Werden private Schlüssel hinterlegt, muss dies im CPS beschrieben werden. Eine Hinterlegung privater Schlüssel durch die PCA erfolgt nicht.

6.2.4 Backup der privaten Schlüssel

Wird ein Backup privater Schlüssel einer CA durchgeführt, so ist dieses auf Datenträgern in einer sicheren Umgebung, z.B. einem Bankschließfach, aufzubewahren. Die privaten Schlüssel müssen durch eine PIN gesichert sein, die jeweils anteilig zur Hälfte den Rollen CAO1 und CAO2 bekannt ist. Schriftliche Kopien der beiden PIN-Hälften werden in versiegelten Umschlägen in einem zweiten Bankschließfach oder bei einem Notar hinterlegt. Der Zugang zu diesen Schließfächern ist streng reglementiert. Wird von diesem Verfahren abgewichen, muss dies im CPS beschrieben werden.

Wird ein Backup privater Schlüssel von Zertifikatnehmern bei der RA oder CA durchgeführt, so muss dies im CPS beschrieben werden.

6.2.5 Archivierung der privaten Schlüssel

Für die Archivierung privater Schlüssel gelten die Regelungen aus Abschnitt 6.2.4.

6.2.6 Transfer privater Schlüssel in ein kryptographisches Modul

Private Schlüssel einer CA, die auf einem IT-System ohne Netzwerkanschluss nach Abschnitt 6.1.1 erzeugt wurden, können nachträglich in ein HSM importiert werden.

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Private Schlüssel einer CA müssen in kryptografischen Modulen immer in verschlüsselter Form abgelegt werden.

6.2.8 Aktivierung der privaten Schlüssel

Bei privaten Schlüsseln einer CA muss die PIN in zwei Hälften unterteilt sein. 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 einer CA muss automatisch nach Beendigung des Zertifizierungsprozesses erfolgen.

6.2.10 Vernichtung der privaten Schlüssel

Bei der Vernichtung der privaten Schlüssel einer CA muss nach dem Vier-Augen-Prinzip verfahren werden. Verantwortlich für die Vernichtung sind die Rollen "ISO" und "CAO1".

6.2.11 Güte des kryptographischen Moduls

Siehe Abschnitt 6.2.1.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Siehe Abschnitt 5.5.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Die in der DFN-PKI ausgestellten Zertifikate haben folgende Gültigkeitsdauer:

- Zertifikate für CAs (auch für die PCA): maximal zwölf Jahre
- Zertifikate für Datenverarbeitungssysteme (Serverzertifikate): maximal fünf Jahre
- Zertifikate für natürliche Personen (Nutzerzertifikate): maximal drei Jahre

Zertifikate können nicht länger gültig sein als das ausstellende CA-Zertifikat.

Für die Nutzungsdauer von Schlüsselpaaren gelten die Regelungen aus Abschnitt 6.1.5.

6.4 Aktivierungsdaten

6.4.1 Aktivierungsdaten für Erzeugung und Installation

Für Passwörter bzw. PINs zur Aktivierung von privaten Schlüsseln müssen nicht triviale Kombinationen aus alphanumerischen Zeichen und Sonderzeichen gewählt werden. Die Länge muss bei der PCA mindestens 15 Zeichen betragen, sonst 8 Zeichen.

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 einer CA dürfen ausschließlich auf Basis von gehärteten Betriebssystemen betrieben werden. Darüber hinaus müssen Zugriffskontrolle und Nutzerauthentifizierung als Sicherheitsmaßnahmen umgesetzt werden.

6.5.2 Güte / Qualität der Sicherheitsmaßnahmen

Die in Abschnitt 6.5.1 genannten Sicherheitsmaßnahmen müssen dem aktuellen Stand der Technik entsprechen.

6.6 Lebenszyklus der Sicherheitsmaßnahmen

Jede CA muss in ihrem CPS den Lebenszyklus der Sicherheitsmaßnahmen beschreiben.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Jede CA muss in ihrem CPS die Sicherheitsmaßnahmen für das Netzwerk beschreiben.

6.8 Zeitstempel

Keine Angaben.

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen

7.1 Zertifikatprofil

7.1.1 Versionsnummer

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

7.1.2 Zertifikaterweiterungen

Grundsätzlich sind alle Zertifikaterweiterungen nach [X.509], [NETS], [PKIX], [PKCS] sowie herstellerspezifische Erweiterungen zulässig.

In Zertifikate für CAs müssen die Erweiterung keyUsage mit den Werten "keyCertSign" und "cRLSign" sowie die Erweiterung basicConstraints mit dem Wert "CA=True" aufgenommen werden.

Zertifikate für alle anderen Verwendungszwecke werden optional mit der Erweiterung basicConstraints mit dem Wert "CA=False" als nicht-CA-Zertifikat markiert und tragen keine CA-spezifische keyUsage-Erweiterung, d.h. die Erweiterung keyUsage darf nicht die Werte "keyCertSign" oder "cRLSign" beinhalten.

Die keyUsage-Erweiterung darf nur mit dem Wert "nonRepudiation" belegt werden, wenn keine Wiederherstellung des privaten Schlüssels möglich ist und der private Schlüssel durch technische und organisatorische Maßnahmen nur dem Zertifikatnehmer zugänglich ist.

7.1.3 Objekt Identifikatoren von Algorithmen

Objekt Identifikatoren für Algorithmen werden nach PKIX verwendet.

7.1.4 Namensformen

Siehe Abschnitt 3.1.

7.1.5 Namensbeschränkungen

Siehe Abschnitt 3.1.

7.1.6 Objekt Identifikator der CP in Zertifikaten

Die folgenden OID können in Abhängigkeit des Sicherheitsniveaus in Zertifikate aufgenommen werden.

Global: Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.4.2.1

Der OID [OID] ist wie folgt zusammengesetzt: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) dfn-verein(22177) pki(300) cp(1) x.509(1) global(4) major-version(2) minor-version(1)}

Classic: Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.1.2.1

Der OID [OID] ist wie folgt zusammengesetzt: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) dfn-verein(22177) pki(300) cp(1) x.509(1) classic(1) major-version(2) minor-version(1)}

Basic: Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.2.2.1

Der OID [OID] ist wie folgt zusammengesetzt: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) dfn-verein(22177) pki(300) cp(1) x.509(1) basic(2) major-version(2) minor-version(1)}

Werden andere als die hier dargestellten OID verwendet, so sind diese im entsprechenden CPS zu beschreiben.

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkung

Keine.

7.1.8 Syntax und Bedeutung von Richtlinienkennungen

Siehe Abschnitt 1.2.

7.1.9 Abarbeitung von kritischen Erweiterungen der CP

Keine.

7.2 CRL Profil

7.2.1 Versionsnummer

Sperrlisten müssen gemäß der internationalen Norm X.509 in der Version 1 oder 2 erstellt werden.

7.2.2 Erweiterungen von CRL und CRL Einträgen

Keine Angaben.

7.3 OCSP Profil

Keine Angaben.

8 Konformitätsprüfung

Jede CA innerhalb der DFN-PKI muss ihre Abläufe so gestalten, dass sie diesem CP und ihrem CPS entsprechen. Jeder CA ist vorbehalten, alle ihr nachgeordneten CAs und RAs auf die Einhaltung der entsprechenden CP und des CPS hin zu überprüfen. Die Überprüfung der PCA erfolgt durch den DFN-Verein.

8.1 Frequenz und Umstände der Überprüfung

Frequenz oder Umstände einer Überprüfung werden durch die zuständige CA festgelegt.

8.2 Identität des Überprüfers

Die zuständige CA kann selbst die Einhaltung der Richtlinien der ihr nachgeordneten CAs und RAs überprüfen. Eine Konformitätsprüfung kann 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 CA 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 prüfenden CA und der überprüften CA bzw. RA behoben werden.

8.6 Veröffentlichung der Ergebnisse

Grundsätzlich erfolgt keine Veröffentlichung der Prüfungsergebnisse.

9 Rahmenvorschriften

9.1 Gebühren

Wenn eine CA Gebühren für ihre Leistungen erhebt, so ist dies in ihrem CPS auszuführen.

9.2 Finanzielle Verantwortung

Versicherungsschutz und Garantie für Sach- und Rechtsmängel sind nicht vorgesehen.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Alle Informationen über Teilnehmer der DFN-PKI, die nicht unter Abschnitt 9.3.2 fallen, werden als vertrauliche Informationen eingestuft.

9.3.2 Nicht vertraulich zu behandelnde Daten

Alle Informationen, die in den herausgegebenen Zertifikaten und Sperrlisten 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 CA trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten dürfen im Rahmen der Diensterbringung 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 CAs und RAs müssen zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten. Dies muss in Übereinstimmung mit den entsprechenden Gesetzen geschehen.

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 CA zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden (siehe Abschnitt 9.4.3) und deren Veröffentlichung nicht widersprochen wurde.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung

Alle innerhalb der DFN-PKI operierenden CAs 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 dieser CP, sowie des CPS der PCA. Die genannten Dokumente können unverändert an Dritte weitergegeben werden. 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 CA verpflichtet sich, alle im Rahmen dieser CP und ihrem CPS beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.2 Verpflichtung der Registrierungsstellen

Jede innerhalb der DFN-PKI operierende RA verpflichtet sich, alle in dieser CP und dem CPS ihrer zugehörigen CA 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 CA in der Verantwortung, den Dienstleister zur Einhaltung der CP und ihres CPS zu verpflichten.

9.7 Gewährleistung

Gewährleistung wird in den Verträgen zwischen den beteiligten Parteien geregelt.

9.8 Haftungsbeschränkung

Haftungsbeschränkung wird in den Verträgen zwischen den beteiligten Parteien geregelt.

9.9 Haftungsfreistellung

Haftungsfreistellung wird in den Verträgen zwischen den beteiligten Parteien geregelt.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Das CP und alle CPS treten an dem Tag in Kraft, an dem sie über den entsprechenden Informationsdienst (siehe Kapitel 2) veröffentlicht werden. Eine Änderung von CP oder CPS der PCA wird vom DFN-Verein angekündigt, Änderungen an weiteren CPS werden von der jeweiligen CA angekündigt.

9.10.2 Aufhebung

Dieses Dokument ist solange gültig, bis es durch eine neue Version ersetzt wird (siehe Abschnitt 9.10.1) oder der Betrieb der durch den DFN-Verein betriebenen CAs eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Von einer Aufhebung der CP oder eines 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 CAs freigestellt.

9.12 Änderungen des Dokuments

Eine Änderung der CP kann nur durch den DFN-Verein erfolgen. Werden Änderungen vorgenommen, die sicherheitsrelevante Aspekte betreffen oder die Abläufe seitens der Zertifikatnehmer erforderlich machen, ist eine Änderung der OID des entsprechenden Dokuments (siehe Abschnitt 1.2) sowie ggf. eine Änderung der OID der CP in Zertifikaten (siehe Abschnitt 7.1.6) erforderlich.

9.13 Konfliktbeilegung

Grundsätzlich ist die in Abschnitt 1.5.2 genannte Stelle für die Konfliktbeilegung zuständig.

9.14 Geltendes Recht

Der Betrieb der DFN-PKI unterliegt den Gesetzen der Bundesrepublik Deutschland.

9.15 Konformität mit dem geltenden Recht

Der DFN-Verein stellt Zertifikate aus, 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 dieser CP oder einem CPS enthaltenen Regelungen gelten zwischen einer innerhalb der DFN-PKI operierenden CA 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 Angaben.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser CP oder eines 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 oder eines CPS vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vorn herein bedacht.

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

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

9.17 Andere Regelungen

Entfällt.

10 Referenzen

[BNA] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, http://www.bundesnetzagentur.de

[IT-GSHB] IT-Grundschutz - die Basis für IT-Sicherheit, http://www.bsi.bund.de/gshb/

[NETS] Netscape Certificate Extensions, Communicator 4.0 Version, http://wp.netscape.com/eng/security/comm4-cert-exts.html

[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)

[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

11 Glossar

Begriff	Erläuterung
CA	--> Zertifizierungsstelle (engl.: Certification Authority)
CN	Bestandteil des DN: Name (engl.: Common Name)
CRL	--> Sperrliste (engl.: Certificate Revocation List)
CP	--> Zertifizierungsrichtlinie (engl.: Certificate Policy)
CPS	--> Erklärung zum Zertifizierungsbetrieb (engl.: Certification Practice Statement)
CSR	--> Zertifikatantrag (engl.: Certificate Signing Request)
DC	Bestandteil des DN: Domain Component
DN	Eindeutiger Name des Zertifikatinhabers oder –ausstellers in Zertifikaten. Ein DN wird aus mehreren Bestandteilen wie z.B. C, O, OU, CN gebildet. (engl.: Distinguished Name)
Erklärung zum Zertifizierungsbetrieb (CPS)	praktische (technisch und organisatorisch) Umsetzung der Zertifizierungsrichtlinie
EXT	Kennzeichen im CN: externe Zertifikatnehmer (engl.: External)
GRP	Kennzeichen im CN: Personen- bzw. Funktionsgruppen (engl.: Group)
HSM	Gerät, das kryptographische Schlüssel sicher speichert und verarbeitet (engl.: Hardware Security Module)
Identifizierung	Personen, die Zertifikate in der DFN-PKI beantragen, müssen ihre Identität feststellen lassen. Dieser Vorgang wird als Identifizierung bezeichnet.
Key Escrow	Schlüsselhinterlegung (siehe Abschnitt 4.12)
Key Recovery	Schlüsselwiederherstellung (siehe Abschnitt 4.12)
LDAP	Protokoll zur Nutzung von Verzeichnisdiensten (engl.: Lightweight Directory Access Protocol)
O	Bestandteil des DN: Organisation
OCSP	Protokoll zur online Prüfung des Status eines Zertifikats (engl.: Online Certification Status Protocol)
Öffentlicher Schlüssel	Schlüssel eines kryptographischen Schlüsselpaares, welcher öffentlich bekannt gemacht wird. Ein öffentlicher Schlüssel kann z.B. zur Überprüfung von elektronischen Signaturen verwendet werden (engl.: Public Key)
OID	Objekt Identifikator – eindeutige Referenz auf ein Objekt in einem Namensraum
OU	Bestandteil des DN: Organisationseinheit (engl.: Organizational Unit)
PCA	Oberste CA einer PKI (engl.: Policy Certification Authority)
PKCS	Serie von kryptografischen Spezifikationen (engl.: Public Key Cryptography Standard) [PKCS]
PKCS#7	Datenaustauschformat zur Übermittlung von Signaturen und verschlüsselten Daten oder auch zur Verteilung von Zertifikaten [PKCS]

Begriff	Erläuterung
PKCS#10	Datenaustauschformat zur Übersendung des öffentlichen Schlüssels und DN eines Zertifikatantrags an eine CA [PKCS]
PKCS#12	Datenaustauschformat zur Speicherung von privatem und öffentlichem Schlüssel, deren Absicherung mit einem Password auf Basis eines symmetrischen Verschlüsselungsverfahrens erfolgt [PKCS]
PKI	--> Zertifizierungsinfrastruktur (engl.: Public Key Infrastructure)
PKIX	Eine Serie von Spezifikationen der IETF im Umfeld von digitalen Zertifikaten nach X.509 Spezifikation [PKIX]
PN	Kennzeichen im CN: Pseudonyme
Privater Schlüssel	Schlüssel eines kryptographischen Schlüsselpaares, welcher nur dem Eigentümer zugänglich ist. Ein privater Schlüssel kann zur Erzeugung von elektronischen Signaturen verwendet werden (engl.: private key)
RA	--> Registrierungsstelle (engl.: Registration Authority)
Registrierung	Vorgang, bei dem eine RA einen Zertifikatantrag prüft und an die zuständige CA weiterleitet (siehe Abschnitt 4.1.2)
Registrierungsstelle (RA)	Wichtigste Aufgabe von Registrierungsstellen ist die Überprüfung der Identität und Authentizität von Zertifikatnehmern
Rezertifizierung	Ausstellen eines neuen Zertifikats unter Beibehaltung des entsprechenden Schlüsselpaares (z.B. zum Ablauf der Gültigkeit eines Zertifikats)
SigG	Deutsches Signaturgesetz [SigG]
Sperrantrag	Wenn ein Zertifikat vor Ablauf der Gültigkeit für ungültig erklärt werden soll, muss ein Sperrantrag für dieses Zertifikat gestellt werden
Sperrliste	Liste aller von einer CA gesperrten Zertifikate
X.509v3	Internationaler Standard für die Definition von Zertifikaten (Version 3) [X.509]
Zertifikat	Zuordnung eines kryptographischen Schlüssels zu einem Namen, die durch die Signatur einer CA bestätigt wird
Zertifikatantrag	Dokument in Papierform oder elektronisch, mit dem bei einer CA die Ausstellung eines Zertifikates beantragt wird. Ein Zertifikatantrag beinhaltet den Namen des Antragstellers, den gewünschten DN im Zertifikat und grundsätzlich den öffentlichen Schlüssel.
Zertifizierungsinfrastruktur (PKI)	Bezeichnung für die notwendigen technischen Einrichtungen sowie der dazugehörenden Prozesse und Konzepte bei der asymmetrischen Kryptographie
Zertifizierungsrichtlinie (CP)	Die Zertifizierungsrichtlinie einer PKI gibt die Regeln vor, an die sich alle Teilnehmer halten müssen. In jeder PKI gibt es genau eine Zertifizierungsrichtlinie.
Zertifizierungsstelle (CA)	Wichtigste Aufgabe von Zertifizierungsstellen ist die Ausstellung von Zertifikaten