deutsches forschungsnetz

Zertifizierungsrichtlinie der DFN-PKI

– Sicherheitsniveau „Global“ –

DFN-Verein
CP der DFN-PKI
V11 14.11.2022

Inhaltsverzeichnis

1 Einleitung 5
1.1 Überblick 5
1.2 Identifikation des Dokuments 5
1.3 An der Zertifizierungsinfrastruktur Beteiligte 5
1.4 Zertifikatnutzung 6
1.5 Verwaltung des Dokuments 6
1.6 Definitionen und Abkürzungen 7
2 Veröffentlichungen und Informationsdienste 7
2.1 Informationsdienste 7
2.2 Veröffentlichung von Informationen 7
2.3 Aktualisierung von Informationen 7
2.4 Zugriff auf Informationsdienste 8
3 Identifizierung und Authentifizierung 8
3.1 Namen 8
3.2 Identitätsüberprüfung bei Neuantrag 11
3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung 13
3.4 Identifizierung und Authentifizierung bei einer Sperrung 14
4 Ablauforganisation 14
4.1 Zertifikatantrag 14
4.2 Bearbeitung von Zertifikatanträgen 14
4.3 Zertifikatausstellung 15
4.4 Zertifikatakzeptanz 15
4.5 Verwendung des Schlüsselpaares und des Zertifikats 15
4.6 Zertifikaterneuerung ohne Schlüsselwechsel 16
4.7 Zertifikaterneuerung mit Schlüsselwechsel 16
4.8 Zertifikatmodifizierung 16
4.9 Sperrung und Suspendierung von Zertifikaten 16
4.10 Dienst zur Statusabfrage von Zertifikaten 18
4.11 Beendigung der Zertifikatnutzung durch den Teilnehmer 18
4.12 Schlüsselhinterlegung und -wiederherstellung 19
5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen 19
5.1 Infrastrukturelle Sicherheitsmaßnahmen 19
5.2 Organisatorische Sicherheitsmaßnahmen 19
5.3 Personelle Sicherheitsmaßnahmen 21
5.4 Sicherheitsüberwachung 21
5.5 Archivierung 21
5.6 Schlüsselwechsel 21
5.7 Kompromittierung und Wiederherstellung 21
5.8 Einstellung des Betriebs 22
6 Technische Sicherheitsmaßnahmen 22
6.1 Schlüsselerzeugung und Installation 22
6.2 Schutz des privaten Schlüssels 23
6.3 Weitere Aspekte des Schlüsselmanagements 24
6.4 Aktivierungsdaten 24
6.5 Sicherheitsmaßnahmen für Computer 25
6.6 Lebenszyklus der Sicherheitsmaßnahmen 25
6.7 Sicherheitsmaßnahmen für das Netzwerk 25
6.8 Zeitstempel 25

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen 25
7.1 Zertifikatprofil 25
7.2 CRL Profil 27
7.3 OCSP Profil 27
8 Konformitätsprüfung 27
8.1 Frequenz und Umstände der Überprüfung 27
8.2 Identität des Überprüfers 27
8.3 Verhältnis von Prüfer zu Überprüftem 27
8.4 Überprüfte Bereiche 28
8.5 Mängelbeseitigung 28
8.6 Veröffentlichung der Ergebnisse 28
9 Rahmenvorschriften 28
9.1 Gebühren 28
9.2 Finanzielle Verantwortung 28
9.3 Vertraulichkeit von Geschäftsinformationen 28
9.4 Schutz personenbezogener Daten (Datenschutz) 28
9.5 Urheberrechte 29
9.6 Verpflichtungen 29
9.7 Gewährleistung 30
9.8 Haftungsbeschränkung 30
9.9 Haftungsfreistellung 30
9.10 Inkrafttreten und Aufhebung 30
9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern 30
9.12 Änderungen des Dokuments 30
9.13 Konfliktbeilegung 30
9.14 Geltendes Recht 30
9.15 Konformität mit dem geltenden Recht 30
9.16 Weitere Regelungen 31
9.17 Andere Regelungen 31
10 Referenzen 31
11 Glossar 32
12 Änderungsverzeichnis 34

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

Dieses Dokument ist die Zertifizierungsrichtlinie (CP) der DFN-PKI für das Sicherheitsniveau Global. Sie regelt die Abläufe und legt dabei insbesondere die Rahmenbedingungen für die Ausstellung von Zertifikaten entsprechend der internationalen Norm X.509 [X.509] fest. Die Regelungen in diesem Dokument beziehen sich ausschließlich auf das Sicherheitsniveau Global der DFN-PKI.

Alle in dieser CP und der Erklärung zum Zertifizierungsbetrieb (CPS) der DFN-PCA angegebenen Regelungen sind für alle Beteiligten der DFN-PKI verbindlich und können nicht abgeschwächt werden. Im CPS wird geregelt, wie die Anforderungen der CP der DFN-PKI im Detail umgesetzt werden.

Im Rahmen der DFN-PKI betreibt der DFN-Verein für das Sicherheitsniveau Global die oberste Zertifizierungsstelle (Policy Certification Authority, DFN-PCA) und alle nachgeordneten Zertifizierungsstellen (Sub-CAs).

CP und CPS in der DFN-PKI sind nach RFC 3647 [RFC3647] gestaltet.

Die DFN-PCA und alle ihre nachgeordneten CAs (Sub-CAs) erfüllen die Anforderungen von ETSI EN 319 411-1 [ETSI319411] nach der OVCP-Policy für Zertifikate für Datenverarbeitungssysteme bzw. nach der NCP-Policy für Zertifikate für Personen.

Die DFN-PCA und alle ihre nachgeordneten CAs (Sub-CAs) erfüllen die Anforderungen der aktuellen Version der unter http://www.cabforum.org veröffentlichten *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* [CAB-BR]. Im Falle einer Inkonsistenz zwischen diesem Dokument und [CAB-BR] gelten die Regelungen aus den [CAB-BR].

1.2 Identifikation des Dokuments

Diese CP ist folgendermaßen identifiziert:

- Titel: Zertifizierungsrichtlinie der DFN-PKI - Sicherheitsniveau Global -
- Version: 11
- Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.4.11

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(11)}

Dieser Object Identifier dokumentiert in den ausgestellten Zertifikaten die Konformität zu [ETSI319411].

1.3 An der Zertifizierungsinfrastruktur Beteiligte

1.3.1 Zertifizierungsstellen

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

Die obersten CAs der DFN-PKI (DFN-PCA) zertifizieren ausschließlich Zertifikate von unmittelbar nachgeordneten CAs entsprechend dieser CP und dem CPS der DFN-PKI. Der Betrieb der DFN-PCA und aller nachgeordneten CAs in der DFN-PKI erfolgt durch den DFN-Verein. Die öffentlichen Schlüssel der DFN-PCA sind im Zertifikat „DFN-Verein Certification Authority 2“ enthalten, das durch die „T-TeleSec GlobalRoot Class 2“ ausgestellt wurde.

Zertifikate für nachgeordnete CAs können in der DFN-PKI ausschließlich durch die DFN-PCA ausgestellt werden. Es gibt eine nachgeordnete CA zur Ausstellung von End-Entity-Zertifika-

ten für die Teilnehmer an der DFN-PKI mit dem Namen „DFN-Verein Global Issuing CA“. Darüber hinaus behält der DFN-Verein sich das Recht vor, für Teilnehmer mit besonderen Anforderungen weitere nachgeordnete Issuing CAs unterhalb der DFN-PCA auszustellen.

1.3.2 Registrierungsstellen

Einer Registrierungsstelle (RA) obliegt die Überprüfung der Identität und Authentizität von Teilnehmern und Zertifikatinhabern. Diese Aufgaben werden von der DFN-PCA übernommen.

Zur Identifizierung natürlicher Personen kann sich die DFN-PCA eines „Teilnehmerservice-Mitarbeiters“ bedienen. Der DFN-PCA liegt eine Liste aller Teilnehmerservice-Mitarbeiter vor.

1.3.3 Teilnehmer

Teilnehmer sind Organisationen, die an der DFN-PKI teilnehmen und eine entsprechende Dienstvereinbarung mit dem DFN-Verein unterzeichnet haben. Diese Organisationen beantragen Zertifikate für Personen und Datenverarbeitungssysteme in ihrem Organisationsbereich. Diese Personen und Datenverarbeitungssysteme sind die Zertifikatinhaber.

Der Kreis der möglichen Teilnehmer ergibt sich aus der Satzung des DFN-Vereins [DFN2000], insbesondere § 2:

„Der Verein fördert die Schaffung der wissenschaftlich-technischen Voraussetzungen für die Errichtung, den Betrieb und die Nutzung eines rechnergestützten Informations- und Kommunikationssystems für die öffentlich geförderte und die gemeinnützige Forschung in der Bundesrepublik Deutschland […].“

1.3.4 Zertifikatprüfer

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

1.3.5 Weitere Beteiligte

Bei Dienstleistern, die für einen Teilnehmer tätig werden, liegt die Verantwortung für die Einhaltung von CP und CPS beim beauftragenden Teilnehmer.

1.4 Zertifikatnutzung

1.4.1 Geeignete Zertifikatnutzung

Die im Rahmen der DFN-PKI ausgestellten Zertifikate dürfen für alle Verfahren genutzt werden, die von dem im Zertifikat enthaltenen Schlüsselverwendungszwecken ermöglicht werden.

Je nach Profil des Zertifikats sind dies unter anderem:

- Authentisierung von Servern mit TLS
- Authentisierung von Nutzern (TLS-Client-Authentisierung)
- Digitale Signatur und Verschlüsselung von E-Mails (S/Mime)
- CodeSigning

Teilnehmer bzw. Zertifikatinhaber sind selbst für die Nutzung in den Anwendungsprogrammen zuständig, sowie für die Prüfung, ob die damit möglichen Anwendungen deren Sicherheitsanforderungen genügen.

1.4.2 Untersagte Zertifikatnutzung

Zertifikatnutzungen, die der Satzung des DFN-Vereins (siehe Abschnitt 1.3.3) widersprechen, sind untersagt.

Die Nutzung des Zertifikats darf nicht im Widerspruch zu den im Zertifikat enthaltenen Schlüsselverwendungszwecken erfolgen, insbesondere 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.

1.5.2 Kontaktperson

Die Kontaktperson für dieses Dokument ist:

DFN-Verein	Telefon: +49 30 884299 955
Dr. Ralf Gröper	Fax: +49 30 884299 70
Alexanderplatz 1	E-Mail: pki@dfn.de (Kein 24x7 Monitoring)
10178 Berlin	WWW: http://www.pki.dfn.de

Kontakt für Notfälle, bei denen Zertifkate aus der DFN-PKI missbräuchlich verwendet werden oder nachweislich kompromittiert sind (Siehe hierzu auch Abschnitt 4.9):

- E-Mail: cert-problems@dfn.de

1.5.3 Verantwortliche Person für Prüfung der CPS

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

1.5.4 Genehmigungsverfahren für CPS

Die Genehmigung der CPS erfolgt durch die Geschäftsführung des DFN-Vereins.

1.6 Definitionen und Abkürzungen

Siehe Kapitel 11.

2 Veröffentlichungen und Informationsdienste

2.1 Informationsdienste

Für jede CA der DFN-PKI werden die in Abschnitt 2.2 genannten Informationen gemäß Abschnitt 2.3 und Abschnitt 2.4 vorgehalten.

2.2 Veröffentlichung von Informationen

Die folgenden Informationen werden veröffentlicht:

- CP der DFN-PKI – Sicherheitsniveau „Global“ –
- CPS der DFN-PKI – Sicherheitsniveau „Global“ –
- Zertifikat der „T-TeleSec GlobalRoot Class 2“ und dessen Fingerabdruck
- Verweis auf die Sperrinformationen der „T-TeleSec GlobalRoot Class 2“
- Zertifikate der DFN-PCA und deren Sub-CAs mit ihren Fingerabdrücken
- Kontaktinformationen, unter denen eine Sperrung beantragt werden kann
- Sperrinformationen der DFN-PCA und ihrer Sub-CAs
- Verweis auf den Verzeichnisdienst der DFN-PKI
- Pflichten der Teilnehmer
- Informationen für Zertifikatinhaber
- Verweise auf die Testwebseiten mit einem gültigen, einem gesperrten und einem abgelaufenen Zertifikat zum Testen der Sperrmechanismen der DFN-PKI

- Diese Informationen werden online auf der Seite https://www.pki.dfn.de/policies/informationen veröffentlicht und stehen dort ständig (24 Stunden am Tag, 7 Tage die Woche) zur Verfügung. Es wird sichergestellt, dass ungeplante Ausfallzeiten und Wartungen minimiert und der Betrieb schnellstmöglich wiederhergestellt wird.

2.3 Aktualisierung von Informationen

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

- Zertifikate: spätestens drei Werktage nach der Ausstellung

- CP und CPS: zum Inkrafttreten einer neuen Version (nach Ankündigung, s. Abschnitt 9.10.1)
- Sperrinformationen:
- CRLs: Siehe Abschnitt 4.9.7
- OCSP: analog zu CRLs (siehe Abschnitt 4.9.7)

2.4 Zugriff auf Informationsdienste

Der lesende Zugriff auf alle in Abschnitt 2.2 aufgeführten Informationen ist ohne Zugriffskontrolle möglich. Schreibender Zugriff auf diese Informationen wird nur berechtigten Personen gewährt.

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 kennzeichnenden Attributen, durch die jeder Zertifikatinhaber eindeutig referenziert wird.

Ein DN entspricht grundsätzlich folgendem Schema, dabei sind optionale Attribute in eckige Klammern gesetzt, Attributwerte in spitzen Klammern müssen durch die jeweiligen Werte ersetzt werden. Die Reihenfolge dieser Attribute muss eingehalten werden. Die Bedeutung der Attribute wird in Abschnitt 3.1.2 beschrieben.

C=<Staat>
[ST=<Bundesland>][1]
[L=<Ort>][1]
O=<Organisation>
[OU=<Organisationseinheit>]
[pseudonym=<Pseudonym>]
[SN=<Nachname>]
[GN=<Vorname>]
CN=<Eindeutiger Name>
[emailAddress=<E-Mail-Adresse>]

Die Attribute „C“ und „O“ müssen genau einmal angegeben werden.

Die Attribute „ST“ und „L“ müssen in Zertifikaten für Datenverarbeitungssysteme (gekennzeichnet durch die in Abschnitt 7.1.6 beschriebenen OIDs) genau einmal angegeben werden, in allen anderen Zertifikaten dürfen die Attribute „ST“ und „L“ jeweils maximal einmal angegeben werden.

Das Attribut „pseudonym“ kann in Pseudonymzertifikaten genau einmal angegeben werden.

Das Attribut SN kann in Zertifikaten für natürliche Personen genau einmal, GN ein- oder keinmal angegeben werden. SN und GN dürfen jeweils 128 Zeichen lang sein.

Die Attribute „OU“ und „emailAddress“ dürfen auch mehrfach angegeben werden.

Weitere Attribute (z. B. „SER“ oder „UID“) können verwendet werden, soweit sie die in der DFN-PKI verwendeten Standards nicht verletzen.

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

In Zertifikate für Datenverarbeitungssysteme werden keine E-Mail-Adressen aufgenommen, weder im DN noch im „subjectAlternativeName“.

---

[1] *Pflichtattribut in Zertifikaten für Datenverarbeitungssysteme*

3.1.2 Aussagekräftigkeit von Namen

Der DN muss den Zertifikatinhaber eindeutig identifizieren und er muss aussagekräftig sein.

Bei der Namensvergabe gelten die folgenden Regelungen:

Das Pflichtattribut „C“ muss das 2-Zeichen-Staaten-Kürzel (festgelegt im ISO Standard 3166-1 [ISO-3166-1]) des Staates enthalten, in dem die im Pflichtattribut „O“ genannte Organisation ihren Standort hat.

Das optionale Attribut[1] „ST“ muss den offiziellen Namen des Bundeslandes enthalten, in dem die im Pflichtattribut „O“ genannte Organisation ihren Standort hat.

Das optionale Attribut[1] „L“ muss den offiziellen Namen des Ortes enthalten, in dem die im Pflichtattribut „O“ genannte Organisation einen Standort hat.

Das Pflichtattribut „O“ muss den Namen des Teilnehmers enthalten. Die Authentizität des Namens wird nach Abschnitt 3.2.2 überprüft.

Falls das optionale Attribut „OU“ ein oder mehrfach angegeben wird, muss es jeweils den Namen einer organisatorischen Untereinheit der im Pflichtattribut „O“ genannten Organisation enthalten. Falls mehrere Attribute „OU“ angegeben werden, müssen diese im DN jeweils direkt hintereinander aufgeführt werden und die Reihenfolge der benannten organisatorischen Untereinheiten sollte von größeren zu kleineren Untereinheiten absteigen.

Der DN enthält exakt ein Attribut „CN“. Das Attribut „CN“ muss eine angemessene Darstellung des Namens des Zertifikatinhabers enthalten. Dabei muss folgendes gelten:

a) Ein Attribut „CN“ in einem Zertifikat für ein Datenverarbeitungssystem enthält alternativ:
   - einen voll-qualifizierten Domain-Namen, dessen Domain bei einem von der ICANN zugelassenen Domain-Namen-Registrar registriert ist. Die Berechtigung, den Namen im Zertifikat verwenden zu dürfen, wird nach Abschnitt 3.2.2 überprüft.
   - eine IP-Adresse, die bei einem von der IANA zugelassenen Internet-Registrar registriert ist. Die Berechtigung, die IP-Adresse im Zertifikat verwenden zu dürfen, wird nach Abschnitt 3.2.2 überprüft.

b) Ein Attribut „CN“ in einem Zertifikat für eine natürliche Person enthält alternativ:
   - Den Namen der Person bestehend aus mindestens einem ausgeschriebenen Vornamen und dem Nachnamen des Zertifikatinhabers; weitere Vornamen und Namenszusätze des Zertifikatinhabers dürfen in ausgeschriebener oder abgekürzter Schreibweise aufgenommen werden oder ganz entfallen. Alle Namen und ggf. Namenszusätze (z. B. „Dr.“) dürfen nur dann aufgenommen werden, wenn diese in dem zur Authentifizierung des Zertifikatinhabers genutzten Ausweisdokument (siehe Abschnitt 3.2.3) enthalten sind. Der Nachname kann ohne Namenszusätze zusätzlich in ein Attribut „SN“ aufgenommen werden, der Vorname in das Attribut „GN“. Gehört der Zertifikatinhaber nicht unmittelbar zum Teilnehmer, so muss dem Namen das Kennzeichen „EXT:“ oder „EXT - “ vorangestellt werden, z. B. „EXT: Dr. Max M. Mustermann“.
   - ein Pseudonym. Bei der Vergabe von Pseudonymen muss eine Verwechslung mit existierenden Namen, z. B. mit natürlichen Personen oder Organisationen, ausgeschlossen werden. Ebenso dürfen keine Domain-Namen, IP-Adressen oder andere innerhalb der DFN-PKI benutzten Syntaxelemente (z. B. „GRP:“, „GRP - “, „EXT: “, „EXT - “) verwendet werden. Ein Pseudonym darf keinen beleidigenden oder anzüglichen Inhalt enthalten. Das Pseudonym muss dem Zertifikatinhaber (authentifiziert nach Abschnitt 3.2.3) eindeutig zugeordnet sein. Das Pseudonym muss mit dem Kennzeichen „PN:“ oder „PN - “ beginnen, z. B. „PN:Deckname“. Das Pseudonym kann ohne die Kennzeichnung „PN:“ oder „PN - “ zusätzlich in ein Attribut „pseudonym“ aufgenommen werden.

c) Ein Attribut „CN“ in einem Zertifikat für eine Personengruppe enthält den Gruppennamen und muss mit dem Kennzeichen „GRP:“ oder „GRP - “ beginnen, z. B. „GRP:Poststelle“. 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 Domain-Namen, IP-Adressen oder andere innerhalb der DFN-PKI benutzten Syntaxelemente (z. B. „PN:“, „PN - “, „EXT:“, „EXT - “) verwendet werden.

d) Ein Attribut „CN“ in einem Zertifikat für eine Zertifizierungsstelle enthält den Namen der CA bzw. einen eindeutigen Hinweis auf die CA-Funktion.

Falls mehrere Attribute „CN“ angegeben werden, müssen diese im DN jeweils direkt hintereinander aufgeführt werden.

Falls das optionale Attribut „emailAddress“ ein- oder mehrfach angegeben wird, muss es jeweils eine nach RFC 822 [RFC822] formatierte E-Mail-Adresse enthalten Die Berechtigung, die E-Mail-Adresse im Zertifikat verwenden zu dürfen, wird nach Abschnitt 3.2.3 geprüft. Falls mehrere Attribute „emailAddress“ angegeben werden, müssen diese im DN jeweils direkt hintereinander aufgeführt werden.

In Zertifikate für Datenverarbeitungssysteme werden keine E-Mail-Adressen aufgenommen, weder im DN noch im „subjectAlternativeName“.

Für E-Mail-Adressen, IP-Adressen und Domain-Namen, die in die Zertifikaterweiterung für alternative Zertifikatnamen („subjectAlternativeName“) unter den Typen „rfc822Name“, „iPAddress“ bzw. „dNSName“ aufgenommen werden, gelten obige Regelungen analog.

Ist ein Attributwert länger als durch den jeweiligen Standard erlaubt, so muss stattdessen eine angemessene, wenn möglich wohlbekannte und eingeführte Abkürzung verwendet werden.

3.1.3 Anonymität und Pseudonymität

Für natürliche Personen kann anstelle des Namens im Zertifikat ein Pseudonym aufgeführt werden. Dieses muss im Attribut „CN“ eindeutig kenntlich gemacht und kann zusätzlich in einem Attribut „pseudonym“ aufgenommen werden (siehe Abschnitt 3.1.2). Das Pseudonym ist dem Zertifikatinhaber (authentifiziert nach Abschnitt 3.2.3) eindeutig zugeordnet. Dies ist in den bei der Beantragung des Zertifikats anfallenden Unterlagen dokumentiert. Das Pseudonym kann somit auf die reale Identität des Zertifikatinhabers zurückgeführt werden.

Anonyme Zertifikate dürfen nicht ausgestellt werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

In den DN-Attributen „ST“, „L“, „O“, „OU“, „SN“, „GN“, „pseudonym“ und „CN“ dürfen ausschließlich

die folgenden Zeichen verwendet werden:

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

Im CN darf für besondere Zertifikattypen zusätzlich ein „*“ verwendet werden.

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 DFN-PCA überprüft werden. Der DN eines Zertifikatinhabers muss eindeutig sein und darf nicht an unterschiedliche Zertifikatinhaber vergeben werden.

Bei Namensgleichheit gilt grundsätzlich das Prinzip: „Wer zuerst kommt, wird zuerst bedient“. In Streitfällen entscheidet die DFN-PCA. Die Eindeutigkeit des DN kann durch die Verwendung von „OU“, „UID“ oder „SER“ Attributen oder durch die Verwendung von Pseudonymen im Attribut „CN“ wie z. B. „PN: Max Mustermann 2“ erreicht werden.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Sofern sich der CN eines Zertifikats auf eine natürliche Person bezieht, ist eine Anerkennung von Warenzeichen o. ä. nicht relevant. In allen anderen Fällen liegt es in der alleinigen Verantwortung des Teilnehmers, dass die Namenswahl keine Warenzeichen o. ä. verletzt. Die DFN-PCA ist nicht verpflichtet, solche Rechte zu überprüfen. Falls sie 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

Bei Antragsstellung muss nachgewiesen werden, dass der zukünftige Zertifikatinhaber im Besitz des privaten Schlüssels ist. Dies geschieht, indem der im Zertifikatantrag enthaltene Certificate Signing Request (CSR) mit dem privaten Schlüssel signiert und an die CA übermittelt wird. Die CA muss die Gültigkeit der Signatur überprüfen.

3.2.2 Authentifizierung einer Organisation

Jede Organisation, die an der DFN-PKI teilnimmt, hat einen DFNInternet-Vertrag mit dem DFN-Verein abgeschlossen. Vor Vertragsschluss werden die von der Organisation gemachten Angaben vom DFN-Verein durch Prüfung geeigneter Unterlagen verifiziert.

Alternativ werden Organisationen durch Vorlage geeigneter Unterlagen wie Registerauszügen oder Landes- und Bundesgesetze oder der Vorlage von Beglaubigungsschreiben (ausgestellt von Rechtsanwälten, Notaren, Buchprüfern oder staatlichen Einrichtungen) authentifiziert. Zertifikate werden ausschließlich für die im Vertrag oder in den beigebrachten Unterlagen genannten Organisationsnamen ausgestellt.

Wird in einem Zertifikat ein Domain-Name (FQDN) oder eine IP-Adresse genutzt, wird das Recht der Organisation, diesen Domain-Namen bzw. diese IP-Adresse zu nutzen, durch den DFN-Verein als Betreiber der DFN-PCA geprüft.

Für die Prüfung von Domain-Namen wird eine der folgenden Methoden eingesetzt:

1. Das Recht der Organisation, für diesen FQDN Zertifikate erhalten zu dürfen, wird durch Versenden eines Zufallswerts per E-Mail, Fax, SMS oder Post und anschließendes Empfangen einer Bestätigungsantwort unter Verwendung des Zufallswerts bestätigt. Der Zufallswert wird an eine E-Mail-Adresse, Fax-/SMS-Nummer oder Postanschrift gesendet, die als Domain-Kontakt identifiziert wurde (Verfahren nach Kapitel 3.2.2.4.2 der [CAB-BR]). Es gilt:
   - Ein(e) E-Mail, Fax, SMS oder Postsendung kann die Berechtigung für mehrere Autorisierungs-Domain-Namen bestätigen.
   - Die DFN-PCA kann die nach diesem Abschnitt erstellte E-Mail, Fax, SMS oder Postsendung an mehr als einen Empfänger senden, vorausgesetzt, dass jeder Empfänger für jeden zu validierenden FQDN vom Registrar des Domain-Namens als Vertreter des Registranten des Domain-Namens aufgeführt wird.
   - Der Zufallswert ist in jeder E-Mail, jedem Fax, jeder SMS oder jeder Postsendung einmalig.
   - Die DFN-PCA kann die gesamte E-Mail, Fax, SMS oder Postsendung, einschließlich der Wiederverwendung des Zufallswertes, erneut versenden, vorausgesetzt, dass der gesamte Inhalt und die Empfänger der Kommunikation unverändert bleiben.
   - Der Zufallswert bleibt für die Verwendung in einer Bestätigungsantwort maximal 30 Tage nach seiner Erstellung gültig.
   - Sobald der FQDN mit dieser Methode validiert wurde, dürfen auch Zertifikate für andere FQDN ausgestellt werden, die mit allen Labels des validierten FQDN enden.
   - Diese Methode wird auch für die Validierung von Wildcard-Domain-Namen eingesetzt.
2. Das Recht der Organisation, für diesen FQDN Zertifikate erhalten zu dürfen, wird bestätigt, indem eine E-Mail an eine oder mehrere Adressen gesendet wird, die unter Verwendung von ‚admin', ‚administrator', ‚webmaster', ‚hostmaster' oder ‚postmaster' als lokalem Teil erstellt wurden, gefolgt von dem At-Zeichen („@"), gefolgt von einem Autorisierungs-Domain-Namen, die einen Zufallswert enthält und die mit einer Antwort unter Verwendung des Zufallswerts bestätigt wurde. (Verfahren nach Kapitel 3.2.2.4.4 der [CAB-BR]). Es gilt:
   - Jede E-Mail kann die Berechtigung für mehrere FQDN bestätigen, vorausgesetzt, dass der in der E-Mail verwendete Autorisierungs-Domain-Name ein Autorisierungs-Domain-Name für jeden FQDN ist, der bestätigt wird.
   - Der Zufallswert ist in jeder E-Mail einmalig.
   - Die E-Mail darf in ihrer Gesamtheit, einschließlich der Wiederverwendung des Zufallswertes, erneut versendet werden, vorausgesetzt, dass ihr gesamter Inhalt und Empfänger unverändert bleiben.

- Der Zufallswert bleibt für die Verwendung in einer Bestätigungsantwort maximal 30 Tage nach seiner Erstellung gültig.
- Sobald der FQDN mit dieser Methode validiert wurde, dürfen auch Zertifikate für andere FQDNs ausgestellt werden, die mit allen Labels des validierten FQDN enden.
- Diese Methode wird auch für die Validierung von Wildcard-Domain-Namen eingesetzt.

Für die Prüfung von IP-Adressen wird eine der folgenden Methoden eingesetzt:

1. Die Kontrolle der Organisation über die IP-Adresse wird bestätigt durch Versenden eines Zufallswerts per E-Mail, Fax, SMS oder Post und anschließendes Empfangen einer Bestätigungsantwort unter Verwendung des Zufallswerts. Der Zufallswert wird an eine E-Mail-Adresse, Fax-/SMS-Nummer oder Postanschrift gesendet, die als IP-Adress-Kontakt identifiziert wurde (Verfahren nach Kapitel 3.2.2.5.2 der [CAB-BR]). Es gilt:
   - Ein(e) E-Mail, Fax, SMS oder Postsendung kann die Berechtigung für mehrere IP-Adressen bestätigen.
   - Die DFN-PCA kann die nach diesem Abschnitt erstellte E-Mail, Fax, SMS oder Postsendung an mehr als einen Empfänger senden, vorausgesetzt, dass jeder Empfänger von der IP-Adress-Registrierungsstelle als IP-Adress-Kontakt zu jeder zu validierenden IP-Adresse aufgeführt wird.
   - Der Zufallswert ist in jeder E-Mail, jedem Fax, jeder SMS oder jeder Postsendung einmalig.
   - Die DFN-PCA kann die gesamte E-Mail, Fax, SMS oder Postsendung auch unter Wiederverwendung des Zufallswertes erneut versenden, vorausgesetzt, dass der gesamte Inhalt und die Empfänger der Kommunikation unverändert bleiben.
   - Der Zufallswert bleibt für die Verwendung in einer Bestätigungsantwort maximal 30 Tage nach seiner Erstellung gültig.
2. Bestätigung der Kontrolle des Antragstellers über die IP-Adresse durch Abfrage eines mit dieser Adresse verbundenen Domain-Namens durch ein Reverse-IP-Lookup und anschließender Prüfung der Kontrolle über den FQDN mit Hilfe der Methoden im obigen Abschnitt. (Verfahren nach Kapitel 3.2.2.5.3 der [CAB-BR])
3. Die Kontrolle der Organisation über die IP-Adresse wird bestätigt durch einen Anruf an die Telefonnummer des IP-Adress-Kontaktes und durch den Erhalt einer Antwort, die die Anfrage der Organisation nach Validierung der IP-Adresse bestätigt. (Verfahren nach Kapitel 3.2.2.5.5 der [CAB-BR]). Es gilt:
   - Der Anruf wird an eine Telefonnummer durchgeführt, die in der IP-Adress-Registrierungsstelle als IP-Adress-Kontakt aufgeführt wird. Jeder Anruf wird an genau eine Telefonnummer getätigt.
   - Wenn jemand anders als der IP-Adress-Kontakt erreicht wird, darf danach gefragt werden, zum IP-Adress-Kontakt durchgestellt zu werden.
   - Wenn nur ein Anrufbeantworter erreicht wird, kann die CA einen Zufallswert und die zu validierende IP-Adresse hinterlassen. Der Zufallswert muss zur Genehmigung der Validierungsanfrage an die CA zurückgeschickt werden.Der Zufallswert bleibt für die Verwendung in einer Bestätigungsantwort maximal 30 Tage nach seiner Erstellung gültig.

Zertifikate für Datenverarbeitungssysteme, die interne IP-Adressen oder interne Namen enthalten, werden nicht ausgestellt[2].

3.2.3 Authentifizierung einer natürlichen Person

- Die Authentifizierung der Identität einer natürlichen Person wird durch die DFN-PCA vorgenommen. Sie kann sich hierzu eines geeigneten Dienstleisters (z. B. PostIdent) bedienen.
- Die Authentifizierung erfolgt durch eine persönliche Identitätsprüfung anhand eines amtlichen gültigen Ausweispapiers mit Lichtbild (Personalausweis oder Reisepass) und wird entsprechend dokumentiert.

---

[2] *Interne IP-Adressen sind in der IANA IPv4 Special-Purpose Address Registry [IANA_IP4] und der IANA IPv6 Special-Purpose Addess Registry [IANA_IP6] gelistet.*

Interne Namen sind in [CAB-BR] definiert.

- Im Falle einer Namensänderung, die im vorgelegten gültigen Ausweisdokument noch nicht berücksichtigt ist, z. B. nach einer Eheschließung, kann zur Authentifizierung zusätzlich zum gültigen Ausweisdokument eine Personenstandsurkunde verwendet werden, die nicht älter als 6 Monate sein darf.

Folgende Informationen müssen 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, oder, falls diese Daten bedingt durch die Art der Identifizierung nicht vorliegen, andere Merkmale, mit denen die Person so weit wie möglich von anderen Personen mit gleichem Namen unterschieden werden kann.
- Name und Anschrift der zugehörigen Organisation
- Nachweis der Zugehörigkeit zur angegebenen Organisation
- Diese Informationen sind für die Zertifikaterstellung notwendig und werden aufgezeichnet. Anhand dieser Daten ist die eindeutige Identifizierung der natürlichen Person möglich.
- E-Mail-Adressen, die in Zertifikate für natürliche Personen oder Personengruppen aufgenommen werden, können auf zwei verschiedene Arten verifiziert werden:
  1. Mit einem Challenge-Response-Verfahren, bei dem an die E-Mail-Adresse, die aufgenommen werden soll, ein Link mit einer individuellen 128-bit langen Zufallszahl geschickt wird, der vom Antragssteller betätigt werden muss, bevor der Antrag genehmigt werden kann.
  2. Oder alternativ durch Abgleich mit einer vom Teilnehmer geführten Adressliste, wenn der Teilnehmer die in das Zertifikat aufzunehmenden E-Mail-Adressen selbst vergibt. Die Domain der E-Mail-Adresse wird bei diesem Verfahren nach den Regeln aus Kapitel 3.2.2 geprüft.

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 Handlungsvollmacht

Jeder Teilnehmer benennt mindestens eine Person, die bevollmächtigt ist, im Namen des Teilnehmers Zertifikate zu beantragen.

Bevollmächtigte Personen belegen die Authentizität von Zertifikatanträgen gegenüber der DFN-PCA entweder durch ihre handschriftliche Unterschrift (Handlungsberechtigte Person), oder durch eine Signatur mit einem eigenen persönlichen Zertifikat (Teilnehmerservice-Mitarbeiter). Der DFN-PCA liegt eine vollständige Liste der Unterschriftenproben der bevollmächtigten Personen sowie eine Liste dieser Zertifikate vor.

Jede bevollmächtigte Person muss nach Abschnitt 3.2.3 authentifiziert werden.

3.2.6 Cross-Zertifizierung

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

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

3.3.1 Routinemäßige Zertifikaterneuerung

Bei der routinemäßigen Zertifikaterneuerung ist neben den Methoden aus Abschnitt 3.2.3 zusätzlich die Authentifizierung der Identität einer natürlichen Person durch ein gültiges persönliches Zertifikat aus der DFN-PKI zulässig, wenn die zugrundeliegende Identifizierung innerhalb der Befristung aus Abschnitt 4.2.1 durchgeführt wurde.

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 (siehe Abschnitt 4.9) kann auf die folgenden Arten erfolgen:

- Übermittlung einer vorher vereinbarten Authentisierungsinformation (schriftlich, per Telefon, oder elektronisch)
- Übergabe eines Sperrantrags mit einer geeigneten elektronischen Signatur, die den Teilnehmer bzw. Zertifikatinhaber authentifiziert
- Übergabe eines Sperrantrags mit einer handschriftlichen Unterschrift

4 Ablauforganisation

4.1 Zertifikatantrag

4.1.1 Wer kann ein Zertifikat beantragen

In der DFN-PKI können Teilnehmer gemäß Abschnitt 1.3.3 Zertifikate beantragen. Hierfür muss für ein Zertifikat für eine natürliche Person deren Autorisierung beim Teilnehmer vorliegen.

4.1.2 Registrierungsprozess

Um ein Zertifikat zu erhalten, muss ein Zertifikatantrag bei einer CA der DFN-PKI eingereicht werden.

Im Registrierungsprozess müssen die folgenden Arbeitsschritte durchlaufen und dokumentiert werden:

- Prüfung des Zertifikatantrags hinsichtlich Vollständigkeit und Korrektheit
- Prüfung des beantragten DN nach Abschnitt 3.1.2 und 3.1.5
- Prüfung des Vorliegens einer Authentifizierung der Identität nach Abschnitt 3.2.3 bei Zertifikaten für natürliche Personen
- Prüfung der Authentifizierung der Organisation nach Abschnitt 3.2.2
- Überprüfung des Besitzes des privaten Schlüssels nach Abschnitt 3.2.1
- Prüfung der Zustimmung zu den Informationen für Zertifikatinhaber und der Datenschutzerklärung
- Bestätigung der Authentizität des Zertifikatantrags durch Prüfung der Bestätigung des Antrags durch eine bevollmächtigte Person, siehe 3.2.5

Angefallene Papierunterlagen müssen archiviert und in einem verschlossenen Schrank aufbewahrt werden. Angefallene digitale Unterlagen müssen archiviert und vor unbefugten Zugriff geschützt aufbewahrt werden.

Die Übermittlung der für die Zertifizierung notwendigen Informationen an die CA erfolgt verschlüsselt und signiert auf elektronischem Weg unter Verwendung des Zertifikats des zuständigen Teilnehmerservice-Mitarbeiters.

4.2 Bearbeitung von Zertifikatanträgen

4.2.1 Durchführung der Identifizierung und Authentifizierung

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

- Für die Authentifizierung einer Organisation gemäß Abschnitt 3.2.2 kann auf bestehende Daten und Dokumente zurückgegriffen werden, wenn die Daten oder Dokumente nicht älter als 825 Tage sind.
- Für die Prüfung der Berechtigung für Domains und IP-Adressen gemäß Abschnitt 3.2.2 kann auf bestehende Daten und Dokumente zurückgegriffen werden, wenn die Daten oder Dokumente nicht älter als 825 Tage, ab dem 01.10.2021 nicht älter als 398 Tage sind.
- Ist der Zertifikatantrag nicht für ein Datenverarbeitungssystem bestimmt, so kann für die Authentifizierung der Identität einer natürlichen Person gemäß Abschnitt 3.2.3 auf bestehende Daten oder Dokumente zurückgegriffen werden, wenn diese nicht älter als 39 Monate sind.

- Für die Authentifizierung der Handlungsvollmacht gemäß Abschnitt 3.2.5 kann auf bestehende Daten oder Dokumente zurückgegriffen werden, wenn diese nicht älter als 39 Monate sind.

4.2.2 Annahme oder Abweisung von Zertifikatanträgen

- Ein Zertifikatantrag wird von der zuständigen CA akzeptiert, wenn alle Arbeitsschritte gemäß Abschnitt 4.1.2 erfolgreich durchlaufen wurden. Andernfalls wird der Zertifikatantrag abgewiesen und dies dem Teilnehmer unter Angabe von Gründen mitgeteilt.
- Bei der Bestätigung eines Antrags durch eine bevollmächtigte Person gemäß Abschnitt 4.1.2 wird bei Zertifikaten für Datenverarbeitungssysteme für jeden enthaltenen Domain-Namen im CN oder in einem dnsName nach dem Verfahren von [RFC6844] geprüft, ob CAA Resource Records im DNS gefunden werden. Wird ein CAA Resource Record gefunden, so wird der Antrag nur freigegeben, wenn die issue- bzw. issuewild-Property den Wert „dfn.de“ oder „pki.dfn.de“ beinhaltet. Wird das Zertifikat nicht innerhalb von 8 Stunden nach der Prüfung ausgestellt, so wird der freigegebene Antrag verworfen.

4.2.3 Bearbeitungsdauer

Bestimmte minimale oder maximale Bearbeitungsdauern sind nicht garantiert.

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 des Teilnehmers, ein Zertifikat für den im DN angegebenen Namen zu erhalten sowie die Gültigkeit der Signatur des Teilnehmerservice-Mitarbeiters.

4.3.2 Benachrichtigung des Teilnehmers nach der Zertifikatausstellung

Nach der Zertifikatausstellung wird dem Teilnehmer sowie ggf. dem Zertifikatinhaber das ausgestellte Zertifikat durch die CA per E-Mail übermittelt oder sie werden über dessen Ausstellung und die Möglichkeit zum Download informiert.

4.4 Zertifikatakzeptanz

Der Zertifikatinhaber 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 angenommen, wenn es verwendet wird oder wenn innerhalb von 14 Tagen nach Erhalt kein Widerspruch erfolgt.

4.4.2 Veröffentlichung des Zertifikats

Die Veröffentlichung von Zertifikaten durch die DFN-PCA erfolgt über den Verzeichnisdienst der DFN-PKI und, im Fall von Zertifikaten für Datenverarbeitungssysteme, über von Dritten betriebene Log-Server des Certificate Transparency Systems. Inhaber von Nutzerzertifikaten haben das Recht, der Veröffentlichung ihres Zertifikats zu widersprechen.

4.4.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist nicht erforderlich.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats

Private Schlüssel müssen angemessen geschützt werden. Zertifikate dürfen ausschließlich in Übereinstimmung mit diesem CP eingesetzt werden.

4.5.2 Pflichten von Zertifikatprüfern

Wenn Zertifikatprüfer Zertifikate aus der DFN-PKI verwenden, müssen sie sicherstellen, dass diese ein im Anwendungskontext angemessenes Sicherheitsniveau haben. Darüber hinaus sind Zertifikatprüfer verpflichtet, sicherzustellen, dass ein geprüftes Zertifikat korrekt und gültig ist. Dies schließt die Prüfung der Signatur des Zertifikats durch die ausstellende CA sowie die Prüfung des Zertifikats auf Sperrung ein.

4.6 Zertifikaterneuerung ohne Schlüsselwechsel

Bei einer Zertifikaterneuerung ohne Schlüsselwechsel wird ein neues Zertifikat unter Beibehaltung des alten Schlüsselpaars ausgestellt, sofern das Schlüsselpaar den kryptographischen Mindestanforderungen der 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 Teilnehmer beantragt.

4.6.3 Ablauf der Zertifikaterneuerung

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

4.6.4 Benachrichtigung des Teilnehmers

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 ein neues Zertifikat für ein neues Schlüsselpaar ausgestellt, sofern die im bereits bestehenden Zertifikat enthaltenen Informationen unverändert bleiben. Es wird analog zu Abschnitt 4.6 vorgegangen.

4.8 Zertifikatmodifizierung

Eine Zertifikatsmodifizierung kann vorgenommen werden, wenn im Zertifikat enthaltene Informationen (z. B. der Verwendungszweck) angepasst werden sollen. Es wird analog zu Abschnitt 4.6 vorgegangen.

4.9 Sperrung und Suspendierung von Zertifikaten

- Kontaktinformationen für Sperranträge werden online unter der Adresse https://www.pki.dfn.de/policies/informationen veröffentlicht. Notfälle, bei denen Zertifikate aus der DFN-PKI missbräuchlich oder betrügerisch verwendet werden oder nachweislich kompromittiert sind, können 24x7 unter der E-Mail-Adresse cert-problems@dfn.de gemeldet werden.
- Bereits abgelaufene Zertifikate können nicht gesperrt werden. Die Sperrung eines Zertifikats kann nicht rückgängig gemacht werden.

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 wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Wenn die Bindung zwischen Subject und Public Key aufgrund von Schwächen in der verwendeten Kryptographie nicht mehr sichergestellt werden kann.
- Der Algorithmus oder ein Paraemter reichen nicht mehr für die geplante Nutzung aus und der erstellte Zeitplan sieht die Sperrung vor.

- Der Zertifikatinhaber ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Das Zertifikat verletzt Warenzeichen o. ä. nach Abschnitt 3.1.6
- Die Nutzung des Zertifikats verstößt gegen die CP oder das CPS.
- Die ausstellende CA stellt den Zertifizierungsbetrieb ein.
- Der Zertifikatinhaber bzw. Teilnehmer stellt einen Sperrantrag.
- Darüber hinaus alle Gründe, die in Kapitel 4.9.1 der Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [CAB-BR] angegeben sind.

4.9.2 Wer kann eine Sperrung beantragen?

Zertifikatinhaber bzw. Teilnehmer können einen Sperrantrag ohne Angabe von Gründen stellen.

Dritte können einen Sperrantrag stellen, wenn sie Hinweise vorlegen, dass einer der unter Abschnitt 4.9.1 genannten Gründe für eine Sperrung vorliegt.

4.9.3 Ablauf einer Sperrung

Stellen Zertifikatinhaber bzw. Teilnehmer einen Sperrantrag, so müssen sie sich gegenüber der ausstellenden CA authentifizieren. Die möglichen Verfahren sind in Abschnitt 3.4 dargestellt. Nach erfolgreicher Authentifizierung führt die ausstellende CA die Sperrung durch.

Stellt ein Dritter einen Sperrantrag, so führt die ausstellende CA eine Prüfung der angegebenen Gründe durch. Liegt einer der in 4.9.1 genannten Gründe vor, führt sie die Sperrung durch.

Nach erfolgter Sperrung werden Teilnehmer und ggf. Zertifikatinhaber darüber elektronisch informiert. Die Sperrinformation wird mindestens bis zum Ablaufdatum des gesperrten Zertifikats über die Sperrdienste verfügbar gemacht.

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

CAs, die nicht ausschließlich CA-Zertifikate ausstellen, müssen mindestens alle 24 Stunden eine neue CRL erstellen und veröffentlichen. Das Datum im Feld nextUpdate dieser CRL darf nicht länger als 10 Tage nach dem thisUpdate-Datum liegen.

Andere CAs müssen mindestens alle 180 Tage eine CRL erstellen und veröffentlichen. Das Datum im Feld nextUpdate dieser CRL darf nicht länger als 12 Monate nach dem thisUpdate-Datum liegen.

Wird ein Zertifikat gesperrt, so muss die sperrende CA umgehend eine neue CRL erstellen und veröffentlichen.

4.9.8 Maximale Latenzzeit für CRLs

Nach Erzeugung neuer CRLs müssen diese umgehend, spätestens jedoch nach 1 Stunde, veröffentlicht werden.

4.9.9 Verfügbarkeit von Online-Sperr- und -Statusüberprüfungsverfahren

CAs können OCSP als Online-Sperr- und -Statusüberprüfungsverfahren anbieten (siehe Abschnitt 4.10). Für alle CAs, die Zertifikate konform zu [CAB-BR] ausstellen, ist dies verpflichtend.

Sperrinformationen werden ständig (24 Stunden am Tag, 7 Tage die Woche) bereitgestellt. Es wird sichergestellt, dass ungeplante Ausfallzeiten und Wartungen minimiert und der Betrieb schnellstmöglich wiederhergestellt werden.

4.9.10 Anforderungen an Online-Sperr- und -Statusüberprüfungsverfahren

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

Die Korrektheit der durch die CA bereitgestellten Sperr- bzw. Statusinformationen über Zertifikate wird durch die allgemeinen Sicherheitsmechanismen der DFN-PCA (siehe Kapitel 5 und 6 sowie CPS) sichergestellt. Auf dem Transportweg sind die Sperr- bzw. Statusinformationen durch elektronische Signaturen gegen Manipulation geschützt (siehe Abschnitte 7.2 und 7.3).

Gesperrte Zertifikate werden sowohl in die zuständige CRL als auch in den OCSP-Dienst eingetragen.

Einträge zu gesperrten Zertifikaten werden nicht vor Ablauf des betroffenen Zertifikats aus der CRL oder dem OCSP-Dienst entfernt.^

Die Systemzeit wird kontinuierlich, spätestens alle 24 Stunden mit der Referenzzeit UTC synchronisiert, z. B. über GPS oder DCF77. Durch Einsatz geeigneter Maßnahmen wird die Genauigkeit und Monotonität der Zeit im Rahmen des Standes der Technik sichergestellt.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrungen

Es gibt keine weiteren Formen der Bekanntmachung von Sperrungen.

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.

Eine Kompromittierung eines privaten Schlüssels kann nachgewiesen werden, indem:

- Mit dem privaten Schlüssel ein PKCS#10-CSR erzeugt wird, der eine klare Kennzeichnung einer Kompromittierung enthält (z.B. den String „The key that signed this CSR has been publicly disclosed.“). Dieser CSR wird dann an die DFN-PCA übermittelt.
- Mit dem privaten Schlüssel ein anderes Artefakt signiert wird, aus dem klar die Kompromittierung hervorgeht. Dieser CSR wird dann an die DFN-PCA übermittelt.
- Der private Schlüssel direkt an die DFN-PCA übermittelt wird (nicht empfohlen).

4.9.13 Gründe für eine Suspendierung

Eine Suspendierung (zeitliche Aussetzung) von Zertifikaten ist nicht erlaubt.

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 zur Bereitstellung von CRLs ist in Kapitel 2 geregelt.

Zertifikate, für die ein Online-Sperr- und -Statusüberprüfungsverfahren (OCSP) angeboten wird, beinhalten einen Verweis auf diesen Dienst. Zertifikate, die den Anforderungen aus [CAB-BR] entsprechen, beinhalten immer einen Verweis auf den OCSP-Dienst.

Der OCSP-Dienst gibt für nicht ausgestellte Zertifikate eine negative Auskunft.

4.11 Beendigung der Zertifikatnutzung durch den Teilnehmer

Eine Beendigung der Zertifikatnutzung erfolgt 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

Die CAs in der DFN-PKI bieten keine Schlüsselhinterlegung und -wiederherstellung für Teilnehmer oder Zertifikatinhaber an. Teilnehmer, die eine interne Schlüsselhinterlegung einsetzen, müssen die im Dokument „Pflichten der Teilnehmer“ angegebenen Vorgaben befolgen.

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 sind im CPS der DFN-PKI in ihren wesentlichen Grundzügen beschrieben. Detaillierte Informationen hierzu sowie zum IT-Sicherheits-Managementprozess sind in einem Sicherheitskonzept festgeschrieben. Darüber hinaus wird regelmäßig eine Risikoanalyse mit Risikobewertung durchgeführt und dokumentiert. Diese werden nicht veröffentlicht, stehen aber im Rahmen der Konformitätsprüfung (siehe Kapitel 8) zur Verfügung. Die Details der Risikoanalyse sind in dem internen Dokument „Risikobewertung des PCA-Betriebs der DFN-PKI“ enthalten. Im Folgenden werden die Maßnahmen für die infrastrukturelle, organisatorische und personelle Sicherheit beschrieben. Details sind im internen Dokument „Betriebshandbuch der DFN-PKI“ enthalten. Das Betriebshandbuch wird an alle Mitarbeitenden der DFN-PCA kommuniziert.

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

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Die infrastrukturellen Sicherheitsmaßnahmen sind für alle CAs im CPS der DFN-PKI beschrieben.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitsrelevante Rollen

In Tabelle 1 sind die sicherheitsrelevanten Rollen definiert, die im Rahmen des Zertifizierungsprozesses erforderlich sind. Um einen ordnungsgemäßen und revisionssicheren Betrieb der DFN-PKI 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.

Rolle	Aufgaben der Rolle	Kürzel
Teilnehmer-service-Mitarbeiter	• Übermittlung von Zertifikatanträgen an die zuständige CA • Übermittlung von Sperranträgen an die zuständige CA • Beratung der Zertifikatinhaber • Durchführung der persönlichen Identifizierung nach Abschnitt 3.2.3 bei Nutzerzertifikaten und Archivierung der zugehörigen Dokumente • TS-Mitarbeiter dürfen Anträge bearbeiten, die sie selber gestellt haben.	TS

Registrierungsstellen-Mitarbeiter	• Entgegennahme von Zertifikat- und Sperranträgen • Prüfung der Autorisierung der Teilnehmer • Prüfung hinsichtlich Vollständigkeit und Korrektheit. • Prüfung der Autorisierung von Domain-Namen • Freigabe von Zertifikat- und Sperranträgen. • Archivierung von Dokumenten	RG
CA-Mitarbeiter	• 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
Revisor	• Durchführung der betriebsinternen Audits • 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 1: Rollen

5.2.2 Erforderliche Anzahl von Personen je Tätigkeit

In Tabelle 2 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. Es wird sichergestellt, dass jede Rolle mit ausreichend vielen Mitarbeitern besetzt ist, um einen kontinuierlichen Betrieb zu gewährleisten.

Tätigkeit	**Rollen**
Freigabe und Übermittlung von Zertifikat- und Sperranträgen für CA-Zertifikate	CAO1 & CAO2
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 2: 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 3 ist aufgeführt, welche Rollen miteinander unverträglich sind.

Rolle	**Unverträglich mit**							
	TS	RG	CAO1	CAO2	SA	SO	R	ISO
TS - Teilnehmerservice-Mitarbeiter					X	X	X	X
RG - Registrierungsstellen-Mitarbeiter					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 - Revisor	X	X	X	X	X	X		
ISO - Sicherheitsbeauftragter	X	X	X	X	X	X		

Tabelle 3: Unverträglichkeit von Rollen

5.3 Personelle Sicherheitsmaßnahmen

Die personellen Sicherheitsmaßnahmen sind für alle CAs im CPS der DFN-PKI beschrieben.

5.4 Sicherheitsüberwachung

Die Maßnahmen zur Sicherheitsüberwachung sind für alle CAs im CPS der DFN-PKI beschrieben.

5.5 Archivierung

Die Maßnahmen zur Archivierung sind für alle CAs im CPS der DFN-PKI beschrieben.

5.6 Schlüsselwechsel

Die Gültigkeitsdauer von Schlüsseln ist in Abschnitt 6.3.2 festgelegt. Falls der Schlüssel einer 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. Die DFN-PCA behandelt jede kritische Schwachstelle, die bisher nicht behandelt wurde, innerhalb einer Frist von 48 Stunden nach ihrer Entdeckung. Wenn ein Sicherheitsvorfall natürliche oder juristische Personen, denen der Dienst zur Verfügung gestellt wurde, mit großer Wahrscheinlichkeit betrifft, so werden diese ohne unnötige Verzögerung informiert.

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 Ersatz-Hardware 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 DFN-PCA 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 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 Teilnehmer bzw. Zertifikatinhaber informiert werden.

Sollten Algorithmen oder Parameter nicht mehr für eine geplante Nutzung ausreichen, werden alle Teilnehmer, Zertifikatprüfern und Zertifikatinhaber informiert. Es wird ein Zeitplan für eine Sperrung der betroffenen Zertifikate erstellt.

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.

Nach einer Katastrophe werden, soweit möglich, Maßnahmen getroffen um eine Wiederholung zu vermeiden.

5.8 Einstellung des Betriebs

Wird der Betrieb einer CA eingestellt, müssen folgende Maßnahmen ergriffen werden:

- Information des Teilnehmers bzw. der Zertifikatinhaber sowie der Zertifikatprüfer
- Sperrung aller von der CA ausgestellten Zertifikate, somit auch aller Zertifikate von Teilnehmerservice-Mitarbeitern
- sichere Zerstörung der privaten Schlüssel der CA
- Widerrufung aller an Auftragnehmer vergebenen Autorisierungen, im Namen der CA zu handeln

Die DFN-PCA muss den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen Sperrliste für den zugesicherten Aufbewahrungszeitraum (siehe CPS der DFN-PKI Abschnitt 5.4.3) sicherstellen.

6 Technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter technischer Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI. Diese Sicherheitsmaßnahmen sind im CPS der DFN-PKI in ihren wesentlichen Grundzügen beschrieben. Detaillierte Informationen sind in einem Sicherheitskonzept festgeschrieben. Im Folgenden werden die Maßnahmen für die technische Sicherheit beschrieben. Details sind im internen Dokument „Betriebshandbuch der DFN-PKI“ enthalten.

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

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Es gibt eine Prozedur für die Erzeugung von Schlüsselpaaren von CAs. Die Dokumentation findet sich im Betriebshandbuch der DFN-PKI und begleitenden Dokumenten.

Die Schlüsselpaare aller CAs müssen in einem Hardware-Sicherheitsmodul (HSM), das den Anforderungen aus Abschnitt 6.2.1 genügt, im Vier-Augen-Prinzip, erzeugt werden (siehe Abschnitt 5.2.2). Die Anzahl der hierzu autorisierten Mitarbeiter wird auf das betrieblich notwendige Maß beschränkt.

Teilnehmer erzeugen ihre Schlüssel selbst und müssen die im Dokument „Pflichten der Teilnehmer“ angegebenen Vorgaben befolgen.

6.1.2 Übermittlung des privaten Schlüssels an den Teilnehmer

Entfällt.

6.1.3 Übermittlung des öffentlichen Schlüssels an den Zertifikatausstеller

Der Certificate Signing Request (CSR) des Teilnehmers 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

Die öffentlichen Schlüssel aller CAs der DFN-PKI können über einen Informationsdienst gemäß Kapitel 2 abgerufen werden.

6.1.5 Schlüssellängen

Bei Einsatz des RSA-Algorithmus müssen alle verwendeten Schlüssel eine Mindestlänge von 2048 Bit haben. Andere Schlüssellängen dürfen verwendet werden, wenn ihre Sicherheit mindestens äquivalent ist.

6.1.6 Parameter der öffentlichen Schlüssel und Qualitätssicherung

Es sind alle kryptographischen Algorithmen entsprechend des Appendix A aus [CAB-BR] zulässig. Alle Zertifikate werden mit SHA-2 unter Verwendung des Paddings nach PKCS#1 v2.1 signiert. Andere Algorithmen dürfen verwendet werden, wenn ihre Sicherheit mindestens äquivalent ist.

CA-Schlüssel dürfen nicht über den aufgrund der Algorithmen erlaubten Gültigkeitszeitraum hinaus verwendet werden.

Bekanntermaßen kompromittierte Schlüssel (z.B. die „Debian weak keys“) oder Schlüssel mit schwachen Parametern wie RSA-Exponenten mit Wert 1 dürfen nicht verwendet werden.

6.1.7 Verwendungszweck der Schlüssel und Beschränkungen

Die privaten Schlüssel der CAs dürfen ausschließlich für die Ausstellung von Zertifikaten und für die Signatur von Sperrinformationen verwendet werden.

6.2 Schutz des privaten Schlüssels

Der private Schlüssel jeder CA muss nicht auslesbar auf einem HSM gespeichert werden. HSMs müssen manipulationssicher transportiert und gelagert werden und korrekt funktionieren

6.2.1 Standard des kryptographischen Moduls

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

- FIPS 140-1 Level 3
- CC EAL4

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 Vier-Augen-Prinzip durch die Rollen CAO1 und CAO2 gemeinsam stattfinden.

6.2.3 Hinterlegung privater Schlüssel (Key Escrow)

Eine Hinterlegung privater Schlüssel durch die DFN-PCA erfolgt nicht.

6.2.4 Backup der privaten Schlüssel

Ein Backup von CA-Schlüsseln wird mit FIPS-140 Level 3 konformen Mechanismen des HSMs durchgeführt, hierbei liegen die CA-Schlüssel in verschlüsselter Form vor. Die Entschlüsselung

kann nur im HSM im Vier-Augen-Prinzip durch die Rollen CAO1 und CAO2 durchgeführt werden. Das Vier-Augen-Prinzip wird durch eine PIN durchgesetzt, die jeweils anteilig zur Hälfte den Rollen CAO1 und CAO2 bekannt ist. Schriftliche Kopien der beiden PIN-Hälften sind in einem versiegelten Umschlag bei einem Notar hinterlegt.

Das Backup der CA-Schlüssel wird in einem Bankschließfach aufbewahrt.

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 werden nach Abschnitt 6.1.1 immer in einem HSM erzeugt.

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

Vor Außerdienststellung eines HSMs müssen alle darauf gespeicherten privaten Schlüssel vernichtet werden. Alle Kopien des privaten Schlüssels einer CA müssen mit Beendigung ihres Lebenszyklus vernichtet werden.

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 DFN-PCA): maximal fünfzehn (15) Jahre
- Zertifikate für Datenverarbeitungssysteme: maximal 398 Tage.
- Zertifikate für natürliche Personen und Gruppen (Nutzerzertifikate): maximal 1185 Tage
- Zertifikate können nicht länger gültig sein als das ausstellende CA-Zertifikat.

Für die Nutzungsdauer von Schlüsselpaaren gelten die Regelungen aus Abschnitt 6.1.6. Bevor der Schlüssel einer CA ungültig wird, wird rechtzeitig ein neues Schlüsselpaar erzeugt und an den notwendigen Stellen bekannt gegeben.

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 für CA-Schlüssel 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.

6.4.3 Weitere Aspekte

Entfällt.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

Alle CAs 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

Für alle CAs ist der Lebenszyklus der Sicherheitsmaßnahmen im CPS der DFN-PKI beschrieben.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Für alle CAs sind die Sicherheitsmaßnahmen für das Netzwerk im CPS der DFN-PKI beschrieben.

6.8 Zeitstempel

Im Rahmen dieses CP wird kein Dienst für Zeitstempel betrieben.

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen

7.1 Zertifikatprofil

Jedem Zertifikat muss durch die ausstellende CA eine eindeutige Seriennummer zugeordnet werden. Die Seriennummer enthält mindestens 64 Bit Zufallsdaten.

7.1.1 Versionsnummer

Zertifikate werden entsprechend der internationalen Norm X.509 in der Version 3 ausgestellt. Alle Zertifikate enthalten folgende Inhalte:

- Identifizierung der ausstellenden CA und des Landes, in dem sie angesiedelt ist
- Der Name des Zertifikatinhabers oder ein entsprechendes Pseudonym
- Der öffentliche Schlüssel, der mit dem privaten Schlüssel unter der Kontrolle des Zertifikatinhabers korrespondiert
- Das Anfangs- und Enddatum der Gültigkeitsperiode des Zertifikats
- Die Seriennummer des Zertifikats
- Die elektronische Signatur der ausstellenden CA
- ggf. Einschränkungen der Einsatzmöglichkeiten des Zertifikats

7.1.2 Zertifikaterweiterungen

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

Zertifikate für CAs

In Zertifikaten für CAs müssen die Erweiterung keyUsage mit den Werten „keyCertSign“ und „cRLSign“ sowie die Erweiterung basicConstraints mit dem Wert „CA=True“ aufgenommen werden. Des weiteren beinhalten Zertifikate für CAs eine Erweiterung cRLDistributionPoint

mit einem Verweis auf die zugehörige Sperrliste und eine Erweiterung authorityInfoAccess mit einem Verweis auf das signierende CA-Zertifikat und den zugehörigen OCSP-Dienst.

End-Entity-Zertifikate

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 Zertifikatinhaber zugänglich ist.

End-Entity-Zertifikate enthalten immer die Erweiterung cRLDistributionPoint mit einem Verweis auf die zugehörige Sperrliste und die Erweiterung authorityInfoAccess mit einem Verweis auf das signierende CA-Zertifikat. Zertifikate für Datenverarbeitungssysteme sowie Zertifikate für natürliche Personen und Gruppen beinhalten zusätzlich immer die Erweiterung authorityInfoAccess mit einem Verweis auf den zugehörigen OCSP-Dienst.

7.1.3 Objekt Identifikatoren von Algorithmen

Objekt Identifikatoren für Algorithmen werden nach PKIX verwendet.

7.1.4 Namensformen

Siehe Abschnitt 3.1.

Domain-Namen und IP-Adressen, die im Subject-DN enthalten sind, werden immer auch in den alternativen Zertifikatnamen („subjectAlternativeName“) unter den Typen „dNSName“ bzw. „iPAddress“ aufgeführt.

7.1.5 Namensbeschränkungen

Siehe Abschnitt 3.1.

7.1.6 Objekt Identifikator der CP in Zertifikaten

Die folgenden OIDs werden in Zertifikate aufgenommen:

Zertifikate für Datenverarbeitungssysteme:

- 1.3.6.1.4.1.22177.300.30: Anzeige der Einhaltung der Baseline Requirements des CA/Browserforums [CAB-BR] (siehe Abschnitt 1.1).
- CA/Browserforum reservierte OID OV 2.23.140.1.2.2
- 1.3.6.1.4.1.22177.300.1.1.4: Anzeige des Sicherheitsniveaus „Global“ und der Konformität zu [ETSI319411].
- OID dieser CP nach Abschnitt 1.2
- OID des für die ausstellende CA gültigen CPS

Zertifikate für andere End-Entity-Zertifikate (nicht für Datenverarbeitungssysteme):

- 1.3.6.1.4.1.22177.300.1.1.4: Anzeige des Sicherheitsniveaus „Global“ und der Konformität zu [ETSI319411].
- OID dieser CP nach Abschnitt 1.2
- OID des für die ausstellende CA gültigen CPS

Zertifikate für CAs:

- 1.3.6.1.4.1.22177.300.30: Anzeige der Einhaltung der Baseline Requirements des CA/Browserforums [CAB-BR] (siehe Abschnitt 1.1).
- 1.3.6.1.4.1.22177.300.1.1.4: Anzeige des Sicherheitsniveaus „Global“ und der Konformität zu [ETSI319411].
- Optional: 1.3.6.1.4.1.22177.300.1.1.4.2.2: OID von CP 2.2
- Optional: 1.3.6.1.4.1.22177.300.1.1.4.3.0: OID von CP 3.0
- Optional: 1.3.6.1.4.1.22177.300.1.1.4.3.1: OID von CP 3.1

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

Für jede CA in der DFN-PKI wird eine CRL bereitgestellt. Diese enthält die gesperrten Zertifikate der jeweiligen CA. Jede CRL enthält folgende Informationen:

- Versionsnummer (siehe Abschnitt 7.2.1)
- Signaturalgorithmus
- Identifizierung der ausstellenden CA
- Zeitpunkt der Ausstellung im Feld thisUpdate
- nextUpdate (Siehe Abschnitt 4.9.7)
- Seriennummern und Sperrungsdaten der gesperrten Zertifikate
- Die elektronische Signatur der ausstellenden CA

7.2.1 Versionsnummer

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

7.2.2 Erweiterungen von CRL und CRL Einträgen

Es werden die Erweiterungen cRLNumber und authorityKeyIdentifier (Variante keyid) gesetzt.

7.3 OCSP Profil

Der OCSP-Dienst wird konform zu [RFC6960] betrieben.

OCSP-Antworten werden mit einem Zertifikat signiert, das von der CA des zu prüfenden Zertifikats ausgestellt wurde.

8 Konformitätsprüfung

Die Abläufe für alle CAs der DFN-PCA sind so gestaltet, dass sie diesem CP und dem CPS der DFN-PKI entsprechen.

8.1 Frequenz und Umstände der Überprüfung

Frequenz und Umstände der Überprüfung ergeben sich aus ETSI EN 319 411-1 [ETSI319411].

8.2 Identität des Überprüfers

Die Überprüfung erfolgt durch einen akkreditierten Auditor gemäß ETSI EN 319 411-1 [ETSI319411].

8.3 Verhältnis von Prüfer zu Überprüftem

Das Verhältnis von Prüfer zu Überprüftem ergibt sich aus Abschnitt 8.2.

8.4 Überprüfte Bereiche

Die von einer Überprüfung betroffenen Bereiche und die Methode der Konformitätsprüfung ergeben sich aus ETSI EN 319 411-1 [ETSI319411].

8.5 Mängelbeseitigung

Aufgedeckte Mängel müssen vom DFN-Verein behoben werden.

8.6 Veröffentlichung der Ergebnisse

Die Veröffentlichung der Prüfungsergebnisse obliegt dem DFN-Verein.

9 Rahmenvorschriften

9.1 Gebühren

Der DFN-Verein erhebt die im Rahmen seiner Dienste üblichen Gebühren für die Nutzung der DFN-PKI.

9.2 Finanzielle Verantwortung

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

9.3 Vertraulichkeit von Geschäftsinformationen

Es wird ein Inventar aller Werte geführt. Den Werten wird eine Klassifikation konsistent mit der Risikobewertung zugewiesen.

9.3.1 Vertraulich zu behandelnde Daten

Alle Informationen über Teilnehmer der DFN-PKI bzw. Zertifikatinhaber, die nicht unter Abschnitt 9.3.2 fallen, werden als vertrauliche Informationen eingestuft. Zertifikatinhaber haben das Recht, Einsicht in die Daten zu erhalten, die bei der Ausstellung ihrer Zertifikate archiviert wurden. Gleiches gilt, im Rahmen der Datenschutzgesetze, für den Teilnehmer.

9.3.2 Nicht vertraulich zu behandelnde Daten

Alle Informationen, die in den veröffentlichten 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

Die DFN-PCA 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 DFN-PCA muss zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten. Dies geschieht in Übereinstimmung mit dem Bundesdatenschutzgesetz (BDSG).

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

Die DFN-PCA nutzt personenbezogene Daten, soweit dies zur Leistungserbringung erforderlich ist.

9.4.6 Offenlegung bei einer gesetzlichen Auskunftspflicht oder einer gerichtlichen Anordnung

Der DFN-Verein unterliegt dem Recht der Bundesrepublik Deutschland und muss vertrauliche und personenbezogene Informationen bei Vorliegen entsprechender gesetzlicher Auskunftspflichten oder bei gerichtlicher Anordnung 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 DFN-PKI. 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

Die DFN-PKI ist ein Dienst des Vereins zur Förderung eines Deutschen Forschungsnetzes e. V. (DFN-Verein). Die DFN-PCA wird von der DFN-CERT Services GmbH (DFN-CERT) im Rahmen eines Dienstleistungsvertrages mit Auftragsdatenverarbeitung betrieben. Der DFN-Verein nimmt die hieraus erwachsenden Prüfpflichten gegenüber dem DFN-CERT wahr und stellt so sicher, dass die vereinbarten Vorgehensweisen umgesetzt werden.

Wenn weitere Auftragnehmer Aufgaben in der DFN-PKI wahrnehmen, so wird durch geeignete Verfahren und Prüfungen sichergestellt, dass die durchgeführten Aufgaben den sich aus CP und CPS der DFN-PKI ergebenden Anforderungen entsprechen. Die Verantwortung für den Betrieb der CAs der DFN-PKI verbleibt beim DFN-Verein.

Der DFN-Verein hat im Rahmen der gesetzlichen Vorschriften adäquate Vorkehrungen für den Fall getroffen, dass er im Falle einer Insolvenz oder aufgrund anderer Gründe nicht mehr in der Lage ist, den in [ETSI319411] geforderten minimalen Fortbetrieb nach Beendigung des CA-Betriebs zu gewährleisten.

Der DFN-Verein hat adäquate Vorkehrungen getroffen, um aus seinen Aktivitäten und Tätigkeiten im Rahmen der DFN-PKI entstehende Verbindlichkeiten bedienen zu können.

Der DFN-Verein hat die finanzielle Stabilität und verfügt über die Ressourcen, um eine CA konform zu den Anforderungen aus [ETSI319411] zu betreiben.

Die Teile der DFN-PCA, die die Ausstellung und Sperrung von Zertifikaten durchführen, verfügen über eine dokumentierte Struktur welche die unbefangene Durchführung der Tätigkeiten gewährleistet.

Die DFN-PCA verpflichtet sich, alle im Rahmen dieser CP und dem CPS der DFN-PKI beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.2 Verpflichtung der Registrierungsstellen

Die DFN-PCA verpflichtet sich, alle in dieser CP und dem CPS der DFN-PKI beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.3 Verpflichtung des Teilnehmers

Jeder Teilnehmer muss eine Dienstvereinbarung mit dem DFN-Verein unterzeichnen. In dieser verpflichtet sich der Teilnehmer insbesondere zum Einhalten dieser CP.

Darüber hinaus müssen die Bestimmungen aus dem Dokument „Pflichten der Teilnehmer“ eingehalten werden. Der Teilnehmer muss außerdem seine Zertifikatinhaber über die Bestimmungen aus dem Dokument „Informationen für Zertifikatinhaber“ informieren und sie verpflichten, diese einzuhalten. Bei Übermittlung des Zertifikats an den Zertifikatinhaber per E-Mail durch die DFN-PCA wird dieses Dokument mit versandt.

9.6.4 Verpflichtung des Zertifikatprüfers

Es gelten die Bestimmungen aus Abschnitt 4.5.2.

9.6.5 Verpflichtung anderer Beteiligter

Sofern weitere Beteiligte als Dienstleister in den Zertifizierungsprozess eingebunden werden, ist die DFN-PCA in der Verantwortung, den Dienstleister zur Einhaltung der CP und des CPS der DFN-PKI 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 das CPS der DFN-PKI treten an dem in ihnen angegebenen Datum in Kraft. Sie werden über den entsprechenden Informationsdienst (siehe Kapitel 2) veröffentlicht. Eine Änderung von CP oder CPS der DFN-PKI wird vom DFN-Verein eine dem Umfang der Änderungen angemessene Zeit, mindestens jedoch zwei Wochen, vorab angekündigt.

Die Geschäftsführung des DFN-Vereins ist verantwortlich für die Implementierung und Einhaltung dieses CP und des CPS der DFN-PKI.

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 DFN-PCA eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Von einer Aufhebung der CP oder des 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 der DFN-PCA freigestellt.

9.12 Änderungen des Dokuments

Eine Änderung der CP kann nur durch die Geschäftsführung des DFN-Vereins erfolgen. Werden Änderungen vorgenommen, die sicherheitsrelevante Aspekte betreffen oder die Abläufe seitens der Teilnehmer erforderlich machen, ist eine Änderung der OID der CP erforderlich (siehe Abschnitt 1.2).

9.13 Konfliktbeilegung

Grundsätzlich ist die in Abschnitt 1.5.2 genannte Stelle für die Konfliktbeilegung zuständig. Kann ein Konflikt von dieser Stelle nicht befriedet werden, kann die Geschäftsführung des DFN-Vereins und bei weiterem Bedarf der Vorstand des DFN-Vereins angerufen werden.

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 in der DFN-PKI Zertifikate aus, mit denen fortgeschrittene elektronische Signaturen gemäß der eIDAS-Verordnung [eIDAS-VO] 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 diesem CP und dem CPS der DFN-PKI enthaltenen Regelungen gelten zwischen dem DFN-Verein und den Beteiligten. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Übertragung der Rechte

Rechte und Pflichten, die aus diesem CP erwachsen, können im Rahmen der üblichen gesetzlichen Vorgaben übertragen werden.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser CP oder des CPS der DFN-PKI 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 dem 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 DFN-Vereins. Der DFN-Verein ist im Vereinsregister des Amtsgerichts Berlin-Charlottenburg unter der Registernummer 7729NZ registriert.

9.17 Andere Regelungen

Die bereitgestellten Dienste werden für Menschen mit Behinderungen zugänglich gemacht, soweit dies möglich ist.

Dieses CP, das CPS, das Sicherheitskonzept und das Verzeichnis der Werte werden jährlich oder bei signifikaten Änderungen überprüft und ggf. angepasst. Änderungen, die Auswirkungen auf das Sicherheitsniveau haben, werden vom Management genehmigt.

10 Referenzen

[CAB-BR] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum, https://cabforum.org/baseline-requirements/

[DFN2000] Satzung des DFN-Vereins, Juli 2000, http://www.dfn.de/fileadmin/6Organisation/Geschaeftsstelle/satzungdfn.pdf

[eIDAS-VO] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910

[ETSI319411] Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, EN 319 411-1

[IANA_IP4] IANA IPv4 Special-Purpose Address Registry, IANA, https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

[IANA_IP6] IANA IPv6 Special-Purpose Address Registry, IANA, https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

[ISO-3166-1] Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm

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

[PKCS] Public Key Cryptography Standards, RSA Security Inc., RSA Laboratories, http://www.rsa.com/rsalabs/pkcs

[PKIX] RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)

[RFC2606] Reserved Top Level DNS Names, Network Working Group, IETF, 1999

[RFC3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003

[RFC6844] DNS Certification Authority Authorization (CAA) Resource Record, P. Hallam-Baker, R. Stradling IETF, 2013

[RFC6960] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, S. Santesson et. al., IETF, 2013

[RFC822] Standard for ARPA Internet Text Messages, David H. Crocker, 1982

[X.509] Information technology - Open Systems Interconnection - The Directory: authentication framework, Version 3, ITU, 1997

11 Glossar

Begriff	Erläuterung
Antragsteller	Antragsteller ist immer ein Teilnehmer (engl.: Applicant)
Autorisierungs-Domain-Name	Der Domain-Name, der verwendet wird, um die Berechtigung zur Ausstellung von Zertifikaten für einen bestimmten FQDN zu erhalten. Die CA kann den von einem DNS CNAME Lookup zurückgegebenen FQDN als FQDN für die Zwecke der Domain-Validierung verwenden. Wenn der FQDN ein Wildcard-Zeichen enthält, dann muss die CA alle Wildcard-Zeichen aus dem linken Teil des angeforderten FQDN entfernen. Die CA kann Null oder mehr Labels von links nach rechts beschneiden, bis sie auf einen Basis-Domain-Namen stößt, und kann einen der Zwischenwerte für die Domain-Validierung verwenden. (engl: Authorization Domain Name)
Basis-Domain-Name	Der Teil eines beantragten FQDN, der der ersten Domain-Namenskomponente links vom durch die Domain-Registry verwalteten oder öffentlichen Domain-Suffix jeweils ergänzt um eben dieses Domain-Suffix entspricht (z.B. "example.co.uk" oder "example.com"). Für FQDNs, bei denen die am weitesten rechts stehende Domain-Namenskomponente eine gTLD ist, in deren ICANN-Registrierungsvereinbarung die Spezifikation 13 ("Marken-TLD-Vereinbarung") aufgenommen ist, kann diese gTLD selbst als Basis-Domain-Name verwendet werden. (engl.: Base Domain Name)
CA	Zertifizierungsstelle (engl.: Certification Authority)
CA-Zertifikat	Zertifikat, von dem weitere Zertifikate (CA- und/oder End-Entity-Zertifikate) ausgestellt werden können
CRL	Sperrliste (engl.: Certificate Revocation List)
CP	Zertifizierungsrichtlinie (engl.: Certificate Policy)
CPS	Erklärung zum Zertifizierungsbetrieb (engl.: Certification Practice Statement)
CSR	Teil des Zertifikatantrags (engl.: Certificate Signing Request)
DFN-PCA	Oberste Zertifizierungsstelle der DFN-PKI (engl.: Policy Certification Authority)
Dienstvereinbarung	Vertragliche Grundlage zur Teilnahme an der DFN-PKI (engl.: Subscriber Agreement)
DN	Eindeutiger Name des Zertifikatinhabers oder -ausstellers in Zertifikaten. (engl.: Distinguished Name)

Begriff	Erläuterung
Domain-Kontakt	Der Registrant des Domain-Namens, technischer Kontakt oder administrativer Kontakt (oder das Äquivalent unter einer ccTLD), wie im WHOIS-Datensatz des Basis-Domain-Namens oder in einem DNS-SOA-Datensatz aufgeführt. (engl.: Domain Contact)
End-Entity-Zertifikat	Alle nicht CA-Zertifikate
Erklärung zum Zertifizierungsbetrieb (CPS)	praktische (technisch und organisatorisch) Umsetzung der Zertifizierungsrichtlinie
EXT	Kennzeichen im CN: externe Zertifikatinhaber (engl.: External)
GRP	Kennzeichen im CN: Personen- bzw. Funktionsgruppen (engl.: Group)
Handlungsberechtigte Person	Eine Handlungsberechtigte Person ist eine vom Teilnehmer benannte Person, die die Leistungen der DFN-PKI beim DFN-Verein im Namen des Teilnehmers beauftragen.
Informationen für Zertifikatinhaber	Informationen zum Umgang mit privaten Schlüsseln für Zertifikatinhaber (engl.: Subject Information)
OCSP	Protokoll zur Online-Prüfung des Status eines Zertifikats (engl.: Online Certificate 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
PCA	Oberste CA einer PKI (engl.: Policy Certification Authority)
PKCS#7	Datenaustauschformat zur Übermittlung von Signaturen und verschlüsselten Daten oder auch zur Verteilung von Zertifikaten [PKCS]
PKCS#10	Datenaustauschformat zur Übersendung des öffentlichen Schlüssels und DN eines Zertifikatantrags (CSR) 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)
PN	Kennzeichen im CN: Pseudonym
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)
Registrierungsstelle	Registrierungsstellen registrieren Teilnehmer einer CA und nehmen Zertifikatanträge für CAs an
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
Teilnehmer	Teilnehmer sind Organisationen, die an der DFN-PKI teilnehmen und eine entsprechendeVereinbarung mit dem DFN-Verein unterzeichnet haben (engl.: Subscriber)

Begriff	Erläuterung
Teilnehmer-service	Der Teilnehmerservice übernimmt in Zusammenhang mit der Ausstellung von Zertifikaten Aufgaben, die sinnvollerweise nur lokal beim Teilnehmer durchgeführt werden können.
Teilnehmerser-vice-Mitarbeiter	Der Teilnehmerservice-Mitarbeiter beantragt Zertifikate für den Teilnehmer. Darüber hinaus berät er Zertifikatinhaber und kann die persönliche Identifizierung im Auftrag der Registrierungsstelle durchführen (engl.: Applicant Representative)
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.
Zertifikatinha-ber	Durch das Subject-Feld des Zertifikats beschriebene Entität, also eine natürliche Person, eine Personengruppe oder ein Datenverarbeitungssystem (engl.: Subject)
Zertifikatname	Synonym: Subject-DN, Name
Zertifikatprüfer	Natürliche oder juristische Person, die sich auf ein Zertifikat verlässt (engl.: Relying Party)
Zertifizierungs-infrastruktur (PKI)	Bezeichnung für die technischen Einrichtungen sowie die dazugehörenden Prozesse und Konzepte bei der asymmetrischen Kryptographie
Zertifizierungs-richtlinie (CP)	Die Zertifizierungsrichtlinie einer PKI gibt die Regeln vor, an die sich alle Beteiligte halten müssen. In jeder PKI gibt es genau eine Zertifizierungsrichtlinie.
Zertifizierungs-stelle (CA)	Wichtigste Aufgabe von Zertifizierungsstellen ist die Ausstellung von Zertifikaten

12 Änderungsverzeichnis

Für weiter zurückliegende Änderungen siehe https://www.pki.dfn.de/policies/policyarchiv

Ver-sion	Änderung	Datum
6	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs 4.9.7 und 7.2: Anpassungen der Regeln zum Ausstellen von Sperrlisten	03.04.2020
7	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs 1.5.2: E-Mail-Adresse für Problem Reports 3.2.2: Validierung von IP-Adressen auch nach Methode 3.2.2.5.3 der BR möglich. Abgelaufene Methode entfernt. 3.2.3: Anpassung an Umstellung von PostIdent 4.9: E-Mail-Adresse, Klarstellung Bearbeitung 6.3.2: Anpassung der Laufzeit von Zertifikaten für Datenverarbeitungssysteme nach Apples Vorgaben ab 01.09.2020 6.4.2: Umstellung des Schutzes von Aktivierungsdaten	03.06.2020

8	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs 1.5.2 und 4.9: Telefonnummer entfernt 4.9.8: Zeitspanne korrigiert 4.9.10: Synchronität zwischen OCSP und CRL Kapitel 8.1-8.4 neu sortiert 5.2.1 Bearbeitung eigener Anträge durch TS-MA konkretisiert 9.17: Accessibility, Aktualisierung CP, Sicherheitskonzept, Assets, Management Approval	30.09.2020
9	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs 3.1.1: SN, GN, pseudonym; CN single-value 3.1.2: SN, GN, pseudonym; CN single-value 3.1.3: Attribut pseudonym 4.2.1: Änderung der Frist zur Wiederverwendung von Daten über die Berechtigungsprüfung bei Domains und IP-Adressen auf 398 Tage ab 1.10.2021 4.9.12: Methoden zum Nachweis der Kompromittierung eines privaten Schlüssels 4.9: Tippfehler entfernt, 9.6.5: Tippfehler Kapitelüberschrift beseitigt, 3.1.2: Tippfehler entfernt	30.06.2021
10	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs 3.2.2: Fußnote korrigiert 10: Referenz IANA Special-Purpose Addresses an Ballot SC48 angepasst	01.10.2021
11	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs 4.1.2: Prüfung der Zustimmung 4.9.1: Sperrgründe ergänzt 4.9.10: Zeitsynchronisation 5: Betriebshandbuch DFN-PCA-intern kommunizieren 5.7.3: Maßnahmen bei Algorithmenproblemen 5.7.4: Maßnahmen zur Vermeidung einer Wiederholung 6.1.1: Prozedur zur Erzeugung von Schlüsselpaaren von CAs 6.2: Funktionsfähigkeit 6.3.2: Gültigkeit von Zertifikaten an Apple Policy angepasst 9.3: Inventar der Werte	14.11.2022