deutsches forschungsnetz

Erklärung zum Zertifizierungsbetrieb der

DFN-Verein Community-PKI

DFN-Verein
CPS der DFN-Verein Community-PKI
V21
22.06.2026~~15. März 2022~~

Kontakt: pki@dfn.de

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.....7
3 Identifizierung und Authentifizierung.....7
3.1 Namen.....7
3.2 Identitätsüberprüfung bei Neuantrag.....10
3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung.....11
3.4 Identifizierung und Authentifizierung bei einer Sperrung.....11
4 Ablauforganisation.....11
4.1 Zertifikatantrag.....11
4.2 Bearbeitung von Zertifikatanträgen.....12
4.3 Zertifikatausstellung.....12
4.4 Zertifikatakzeptanz.....12
4.5 Verwendung des Schlüsselpaares und des Zertifikats.....13
4.6 Zertifikaterneuerung ohne Schlüsselwechsel.....13
4.7 Zertifikaterneuerung mit Schlüsselwechsel.....13
4.8 Zertifikatmodifizierung.....13
4.9 Sperrung und Suspendierung von Zertifikaten.....14
4.10 Dienst zur Statusabfrage von Zertifikaten.....15
4.11 Beendigung der Zertifikatnutzung durch den Teilnehmer.....15
4.12 Schlüsselhinterlegung und -wiederherstellung.....15
5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen.....15
5.1 Infrastrukturelle Sicherheitsmaßnahmen.....15
5.2 Organisatorische Sicherheitsmaßnahmen.....16
5.3 Personelle Sicherheitsmaßnahmen.....17
5.4 Sicherheitsüberwachung.....18
5.5 Archivierung.....18
5.6 Schlüsselwechsel.....19
5.7 Kompromittierung und Wiederherstellung.....19
5.8 Einstellung des Betriebs.....19
6 Technische Sicherheitsmaßnahmen.....20
6.1 Schlüsselerzeugung und Installation.....20
6.2 Schutz des privaten Schlüssels.....20
6.3 Weitere Aspekte des Schlüsselmanagements.....21
6.4 Aktivierungsdaten.....21
6.5 Sicherheitsmaßnahmen für Computer.....21
6.6 Lebenszyklus der Sicherheitsmaßnahmen.....22
6.7 Sicherheitsmaßnahmen für das Netzwerk.....22
6.8 Zeitstempel.....22

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen.....22
7.1 Zertifikatprofil.....22
7.2 CRL Profil.....23
7.3 OCSP Profil.....24
8 Konformitätsprüfung.....24
8.1 Frequenz und Umstände der Überprüfung.....24
8.2 Identität des Überprüfenden.....24
8.3 Verhältnis von Prüfenden zu Überprüftem.....24
8.4 Überprüfte Bereiche.....24
8.5 Mängelbeseitigung.....24
8.6 Veröffentlichung der Ergebnisse.....24
9 Rahmenvorschriften.....24
9.1 Gebühren.....24
9.2 Finanzielle Verantwortung.....24
9.3 Vertraulichkeit von Geschäftsinformationen.....25
9.4 Schutz personenbezogener Daten (Datenschutz).....25
9.5 Urheberrechte.....25
9.6 Verpflichtungen.....25
9.7 Gewährleistung.....26
9.8 Haftungsbeschränkung.....26
9.9 Haftungsfreistellung.....26
9.10 Inkrafttreten und Aufhebung.....26
9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern.....26
9.12 Änderungen des Dokuments.....26
9.13 Konfliktbeilegung.....26
9.14 Geltendes Recht.....26
9.15 Konformität mit dem geltenden Recht.....26
9.16 Weitere Regelungen.....26
9.17 Andere Regelungen.....27
10 Referenzen.....28
11 Glossar.....28
12 Änderungsverzeichnis.....30

1 Einleitung

Der Verein zur Förderung eines Deutschen Forschungsnetzes e. V. (DFN-Verein) betreibt das Deutsche Forschungsnetz (DFN) und stellt seine Weiterentwicklung und Nutzung sicher. Dieses Hochleistungsnetz für Wissenschaft und Forschung verbindet Hochschulen und Forschungseinrichtungen miteinander und unterstützt 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 https://www.pki.dfn.de abrufbar.

1.1 Überblick

Dieses Dokument ist die Erklärung zum Zertifizierungsbetrieb (CPS) der DFN-Verein Community PKI. Es regelt die Abläufe und setzt die Rahmenbedingungen für die Ausstellung von Zertifikaten für Personen und Datenverarbeitungssysteme nach der Norm X.509 [X.509] fest. Die in diesem CPS angegebenen Regelungen sind für alle Beteiligten der DFN-Verein Community-PKI verbindlich.

Die Policy Certification Authority (DFN-PCA) des DFN-Vereins betreibt die oberste Zertifizierungsstelle (Root-CA) und alle nachgeordneten Zertifizierungsstellen (Sub-CAs) der DFN-Verein Community-PKI. Der DFN-Verein hat die DFN-CERT Services GmbH mit dem Betrieb der DFN-PCA beauftragt.

Die DFN-Verein Community-PKI dient der Etablierung eines gemeinsamen Sicherheitsniveaus für die Kommunikation der Teilnehmer des DFN-Vereins untereinander und für deren interne Zwecke. Sie wird für Anwendungsfälle verwendet, in denen die Verankerung in den Root-Programmen gängiger Softwarehersteller nicht notwendig ist.

Die DFN-Verein Community-PKI dient nicht der Authentifizierung öffentlich zugänglicher Server.

Dieses CPS ist nach RFC 3647 [RFC3647] gestaltet.

1.2 Identifikation des Dokuments

Dieses CPS hat folgende Kennzeichnung:

- Titel: Erklärung zum Zertifizierungsbetrieb der DFN-Verein Community-PKI
- Version: 2~~1~~
- Object Identifier (OID): 1.3.6.1.4.1.22177.300.2.1.7.~~1~~2

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) cps(2) x.509(1) community(7) major-version(~~1~~2)}

1.3 An der Zertifizierungsinfrastruktur Beteiligte

1.3.1 Zertifizierungsstellen

Die folgende Root-CA ist im Gültigkeitsbereich dieses CPS:

Name:	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V. /OU=DFN-PKI/CN=DFN-Verein Community Root CA 2022
Schlüssellänge:	RSA 4096 Bit
Gültigkeit:	Jan 26 14:08:41 2022 GMT bis Jan 21 14:08:41 2042 GMT
SHA256-Fingerprint:	3C:DC:2C:9E:9E:5A:36:CB:58:88:FD:17:96:CB:91:2F:84:62:53:B6:82:C1:B3:20:57:53:20:33:51:0C:7B:B6

Zertifikate für Personen und Datenverarbeitungssysteme werden nicht von der Root-CA, sondern ausschließlich von Sub-CAs ausgestellt.

1.3.2 Registrierungsstelle und Teilnehmerservice

Die Registrierungsstelle (RA) überprüft die Identität und Authentizität von Teilnehmern und Zertifikatinhabenden. Die DFN-PCA ist die Registrierungsstelle in der DFN-Verein Community-PKI.

Die Identifizierung natürlicher Personen und die Verifikation von E-Mail-Adressen kann durch einen Teilnehmerservice bei den teilnehmenden Organisationen durchgeführt werden.

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 Zertifikatinhabenden.

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 Zertifikatprüfende

Zertifikatprüfende sind natürliche Personen und Organisationen, die unter Nutzung eines innerhalb der DFN-Verein Community-PKI ausgestellten Zertifikats die Authentizität von Personen oder Datenverarbeitungssystemen überprüfen.

1.3.5 Weitere Beteiligte

Keine Angaben.

1.4 Zertifikatnutzung

1.4.1 Geeignete Zertifikatnutzung

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

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

1.5 Verwaltung des Dokuments

1.5.1 Organisation

Die Verwaltung dieses Dokuments erfolgt durch die DFN-PCA.

1.5.2 Kontaktperson

DFN-Verein	Telefon: +49 30 884299 955
DFN-PKI	
Alexanderplatz 1	E-Mail: pki@dfn.de (kein 24/7 Monitoring)
10178 Berlin	WWW: https://www.pki.dfn.de

1.5.3 Verantwortliche Person für Prüfung der CPS

Die in Abschnitt 1.5.2 benannte Stelle ist für die Prüfung des CPS der DFN-Verein Community-PKI verantwortlich.

1.5.4 Genehmigungsverfahren für CPS

Die Genehmigung dieses CPS erfolgt durch die Leitung der DFN-PCA.

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 unter https://www.pki.dfn.de/dfn-verein-community-pki veröffentlicht:

- CPS der DFN-Verein Community-PKI
- Root-CA-Zertifikat "DFN-Verein Community Root CA 2022" und deren Sub-CAs mit ihren Fingerabdrücken

2.3 Aktualisierung von Informationen

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

- CPS: zum Inkrafttreten einer neuen Version
- CA-Zertifikate: spätestens 14 Tage nach der Ausstellung
- Sperrinformationen:
  - CRLs: Siehe Abschnitt 4.9.7
  - OCSP: analog zu CRLs (siehe Abschnitt 4.9.7)

2.4 Zugriff auf Informationsdienste

Auf die in Abschnitt 2.2 aufgeführten Informationen kann öffentlich ohne Beschränkung zugegriffen werden. Diese Informationen können nur von der DFN-PCA modifiziert werden.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensform

Ein eindeutiger Name (DN) entspricht grundsätzlich dem folgenden Schema. Optionale Attribute sind in eckige Klammern gesetzt.

C=<Staat>
ST=<Bundesland>
L=<Ort>
O=<Organisation>
[OU=<Organisationseinheit>]
[CN=<Eindeutiger Name>]
[emailAddress=<E-Mail-Adresse>]

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

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

Weitere Attribute (z. B. „SN“, „GN“ oder „SER“) können verwendet werden.

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“.

3.1.2 Aussagekräftigkeit von Namen

Der DN muss den Antragstellenden 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 Pflichtattribut „ST“ muss den offiziellen Namen des Bundeslandes enthalten, in dem die im Pflichtattribut „O“ genannte Organisation ihren Standort hat.
- Das Pflichtattribut „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.

Für das Attribut „CN“ gelten die folgenden Regeln:

CN in Zertifikaten für Datenverarbeitungssysteme

Das Attribut „CN“ muss entweder genau einmal angegeben werden oder ganz entfallen. Wenn es nicht angegeben ist, enthält die Zertifikaterweiterung subjectAlternativeName mindestens einen Wert vom Typ „iPAddress“ oder „dNSName“.

Das Attribut „CN“, sofern angegeben, und/oder subjectAlternativeName können enthalten:

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

~~Ein Attribut „CN“ in einem Zertifikat für ein Datenverarbeitungssystem enthält alternativ:~~

- ~~einen~~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~~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.

CN in Zertifikaten für natürliche Personen

Das~~Ein~~ Attribut „CN“ wird exakt einmal angegeben und ~~in einem Zertifikat für eine natürliche Person~~ enthält alternativ:

- Den Namen der Person bestehend aus mindestens einem ausgeschriebenen Vornamen und dem Nachnamen; weitere Vornamen und Namenszusätze dürfen in ausgeschriebener oder abgekürzter Schreibweise aufgenommen werden oder ganz entfallen.
- ~~ein~~Ein Pseudonym. Das Pseudonym muss den Zertifikatinhabenden (authentifiziert nach Abschnitt 3.2.3) eindeutig zugeordnet sein. Das Pseudonym muss mit dem Kennzeichen „PN:“ oder „PN - “ beginnen, z. B. „PN:Deckname“.

CN in Zertifikaten für Personengruppen

~~Ein~~Das Attribut „CN“ wird exakt einmal angegeben und~~in einem Zertifikat für eine Personengruppe~~ enthält den Gruppennamen. ~~Dieser~~ ~~und~~ muss mit dem Kennzeichen „GRP:“ oder „GRP - “ beginnen, z. B. „GRP ~~- :~~Poststelle“.

CN in Zertifikaten für Zertifizierungsstellen

~~Ein~~Das Attribut „CN“ wird exakt einmal angegeben und~~in einem Zertifikat für eine Zertifizierungsstelle~~ enthält den Namen der CA bzw. einen eindeutigen Hinweis auf die CA-Funktion.

E-Mail-Adressen

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.

Für E-Mail-Adressen, die in die Zertifikaterweiterung für alternative Zertifikatnamen („subjectAlternativeName“) unter dem Typ „rfc822Name“ aufgenommen werden, gelten obige Regelungen analog.

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

Zertifikaterweiterung für alternative Zertifikatnamen („subjectAlternativeName“)

~~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.~~Zertifikaterweiterungen für alternative Zertifikatnamen („subjectAlternativeName“) vom Typ „dNSName“ müssen einen voll-qualifizierten Domain-Namen, dessen Domain bei einem von der ICANN zugelassenen Domain-Namen-Registrar registriert ist, enthalten. Die Berechtigung, den Namen im Zertifikat verwenden zu dürfen, wird nach Abschnitt 3.2.2 überprüft.

Zertifikaterweiterungen für alternative Zertifikatnamen („subjectAlternativeName“) vom Typ „iPAddress“ müssen eine IP-Adresse, die bei einem von der IANA zugelassenen Internet-Registrar registriert ist, enthalten. Die Berechtigung, die IP-Adresse im Zertifikat verwenden zu dürfen, wird nach Abschnitt 3.2.2 überprüft.

Abkürzungen von Attributwerten

Ist ein Attributwert länger als durch den jeweiligen Standard erlaubt, so muss stattdessen eine konforme angemessene 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 werden (siehe Abschnitt 3.1.2). Das Pseudonym ist dem Zertifikatinhabenden (authentifiziert nach Abschnitt 3.2.3) eindeutig zugeordnet. Die Zuordnung muss bei der Beantragung des Zertifikats dokumentiert werden. Das Pseudonym kann somit auf die reale Identität der das Zertifikat innehabenden Person zurückgeführt werden.

Anonyme Zertifikate dürfen nicht ausgestellt werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

In den DN-Attributen „ST“, „L“, „O“, „OU“ 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, 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/einer Zertifikatinhaberin muss eindeutig sein und darf nicht an unterschiedliche Personen vergeben werden.

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

Es liegt in der alleinigen Verantwortung des Teilnehmers, dass die Namenswahl keine Warenzeichen o. ä. verletzt. Die DFN-PCA ist nicht verpflichtet, solche Rechte zu überprüfen. Eine Verletzung solcher Rechte kann ein Grund zur Sperrung des Zertifikats sein.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Bei Antragsstellung muss nachgewiesen werden, dass der Antragsstellende im Besitz des privaten Schlüssels ist. Dies geschieht, indem der im Zertifikatantrag enthaltene Certificate Signing Request (CSR) mit dem privaten Schlüssel signiert ist. Die CA überprüft die Gültigkeit der Signatur.

3.2.2 Authentifizierung einer Organisation

Jede Organisation, die an der DFN-PKI teilnimmt, hat einen 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 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 die 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 und anschließendes Empfangen einer Bestätigungsantwort unter Verwendung des Zufallswerts bestätigt. Der Zufallswert wird an eine E-Mail-Adresse gesendet, die als Domain-Kontakt identifiziert wurde (Verfahren nach Kapitel 3.2.2.4.2 der [CAB-BR]).
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]).

Für die Prüfung von IP-Adressen wird die folgende Methoden eingesetzt:

1. 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])

Zertifikate für Datenverarbeitungssysteme, die interne IP-Adressen oder interne Namen enthalten, werden nicht ausgestellt[1].

[1] *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.*

3.2.3 Authentifizierung einer natürlichen Person

Die Authentifizierung der Identität einer natürlichen Person, deren Namen in einem Zertifikat aufgenommen werden soll, muss nach einem Verfahren vorgenommen werden, dass mindestens den Anforderungen des REFEDS Assurance Frameworks an Identity Proofing im Level Low entsprechen [REFEDS_RAF].

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 Antragsstellenden 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.

3.2.6 Kriterien zur Interoperabilität

Keine Angaben.

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 durch eine Signatur durch ein gültiges persönliches Zertifikat aus der DFN-PKI zulässig.

3.3.2 Zertifikaterneuerung nach einer Sperrung

Nach dem Sperren eines Zertifikats kann eine Authentifizierung nicht mehr mit dem gesperrten Zertifikat durchgeführt werden. Wurde das Zertifikat aufgrund einer Kompromittierung des privaten Schlüssels gesperrt, kann es nicht mehr mit demselben Schlüssel erneuert 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. Zertifikatinhabenden authentifiziert
- Übergabe eines Sperrantrags mit einer handschriftlichen Unterschrift

4 Ablauforganisation

4.1 Zertifikatantrag

4.1.1 Wer kann ein Zertifikat beantragen

Teilnehmer gemäß Abschnitt 1.3.3 können Zertifikate beantragen.

Interne Namen sind in [CAB-BR] definiert.

4.1.2 Registrierungsprozess

Wenn ein Zertifikatantrag bei einer CA der DFN-Verein Community-PKI eingereicht wurde, werden die folgenden Arbeitsschritte durchlaufen und dokumentiert:

- 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
- Prüfung der Authentifizierung der Organisation nach Abschnitt 3.2.2
- Überprüfung des Besitzes des privaten Schlüssels nach Abschnitt 3.2.1
- Bestätigung der Authentizität des Zertifikatantrags durch Prüfung der Freigabe des Antrags durch eine bevollmächtigte Person, siehe 3.2.5

Angefallene digitale Unterlagen werden bei der DFN-PCA archiviert.

4.2 Bearbeitung von Zertifikatanträgen

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die Identifizierung und Authentifizierung von Antragsstellenden werden gemäß Abschnitt 3.2 durchgeführt.

Für die Authentifizierung einer Organisation gemäß Abschnitt 3.2.2 kann auf bestehende Daten und Dokumente zurückgegriffen werden.

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 1185 Tage (ca. 39 Monate) alt 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.

Für die Authentifizierung der Handlungsvollmacht gemäß Abschnitt 3.2.5 kann auf bestehende Daten oder Dokumente zurückgegriffen werden.

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.

Es werden keine CAA Ressource Records im DNS nach [RFC6844] geprüft.

4.2.3 Bearbeitungsdauer

Bestimmte minimale oder maximale Bearbeitungsdauern werden 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 (siehe Abschnitt 1.3.2).

4.3.2 Benachrichtigung des Teilnehmers nach der Zertifikatausstellung

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

4.4 Zertifikatakzeptanz

Zertifikatinhabende sind verpflichtet, die Korrektheit des eigenen Zertifikats nach Erhalt zu verifizieren.

4.4.1 Annahme des Zertifikats

Ein Zertifikat wird angenommen, indem es verwendet wird.

4.4.2 Veröffentlichung des Zertifikats

Die Veröffentlichung von Zertifikaten erfolgt über den Verzeichnisdienst der DFN-PKI (siehe Kapitel 2). Zertifikatinhabende müssen der Veröffentlichung ihres Zertifikats zustimmen.

Es erfolgt keine Veröffentlichung von Zertifikaten in Log-Server des Certificate Transparency Systems.

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 CPS eingesetzt werden.

4.5.2 Pflichten von Zertifikatprüfenden

Wenn Zertifikatprüfende Zertifikate aus der DFN-PKI verwenden, müssen sie sicherstellen, dass diese ein im Anwendungskontext angemessenes Sicherheitsniveau haben. Darüber hinaus sind Zertifikatprüfende 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 des CPS genügt, die im Zertifikat enthaltenen Informationen unverändert bleiben und das bestehende Zertifikat nicht wegen einer Kompromittierung des privaten Schlüssels gesperrt wurde.

4.6.1 Gründe für eine Zertifikaterneuerung

Eine Zertifikaterneuerung kann jederzeit beantragt werden.

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

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, offengelegt oder anderweitig kompromittiert bzw. missbraucht.
- Der Zertifikatinhabende 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 Zertifikatinhabende bzw. Teilnehmer stellt einen Sperrantrag.

4.9.2 Wer kann eine Sperrung beantragen?

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

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

4.9.3 Ablauf einer Sperrung

Stellen Zertifikatinhabende 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. Zertifikatinhabende darüber elektronisch informiert. Die Sperrinformation wird mindestens bis zum Ablaufdatum des gesperrten Zertifikats verfügbar gemacht.

4.9.4 Fristen für Stellung eines Sperrantrags

Wenn Gründe für eine Sperrung (siehe Abschnitt 4.9.1) 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 Zertifikatprüfende

Siehe Abschnitt 4.5.2.

4.9.7 Veröffentlichungsfrequenz für CRLs

Sub-CAs erstellen alle 24 Stunden eine neue CRL und veröffentlichen diese. Das Datum im Feld nextUpdate dieser CRL darf nicht länger als 10 Tage nach dem thisUpdate-Datum liegen.

Die Root-CA muss 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 werden diese umgehend, spätestens jedoch nach 24 Stunden, veröffentlicht.

4.9.9 Verfügbarkeit von Online-Sperr- und -Statusüberprüfungsverfahren

Als Online-Sperr- und -Statusüberprüfungsverfahren ist OCSP verfügbar (siehe auch Abschnitt 4.10).

4.9.10 Anforderungen an Online-Sperr- und -Statusüberprüfungsverfahren

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

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.

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.

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

Zertifikate, für die ein Online-Sperr- und -Statusüberprüfungsverfahren (OCSP) angeboten wird, beinhalten einen Verweis auf diesen 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-Verein Community-PKI bieten keine Schlüsselhinterlegung und -wiederherstellung für Teilnehmer oder Zertifikatinhabende an. Teilnehmer können eine interne Schlüsselhinterlegung einsetzen.

4.12.2 Richtlinien und Praktiken zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung

Entfällt.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Die infrastrukturellen Sicherheitsmaßnahmen sind in einem internen Sicherheitskonzept beschrieben.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitsrelevante Rollen

In Tabelle 1 sind die sicherheitsrelevanten Rollen des Zertifizierungsprozesses der DFN-Verein Community-PKI definiert.

Rolle	Aufgaben der Rolle	Kürzel
Teilnehmerservice-Mitarbeitende	• Übermittlung von Zertifikatanträgen an die zuständige CA • Übermittlung von Sperranträgen an die zuständige CA • Beratung der Zertifikatinhabenden • Durchführung der persönlichen Identifizierung nach Abschnitt 3.2.3 bei Nutzerzertifikaten	TS
CA-Mitarbeitende	• Prüfung der Autorisierung der Teilnehmer • Prüfung hinsichtlich Vollständigkeit und Korrektheit. • Prüfung der Autorisierung von Domain-Namen • Freigabe von Zertifikat- und Sperranträgen. • 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
Systemadministrator/-in	• Kenntnis der zweiten Hälfte der PINs der privaten Schlüssel der CA. • 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. • Betreuung der Datensicherung und –wiederherstellung der erforderlichen Server und der CA-Anwendungssoftware.	CAO2
Revisor/-in	• Durchführung der betriebsinternen Audits • Überwachung und Einhaltung der Datenschutzbestimmungen.	R
Sicherheitsbeauftragte/-r	• 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 Mitarbeitenden 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

Tätigkeit	Rollen
Starten von Prozessen zur Ausstellung von Zertifikaten und Sperrlisten	CAO1 & CAO2
Austausch von Hard- und Softwarekomponenten für die Zertifizierung	CAO1 & CAO2

Tabelle 2: Tätigkeiten, die das Vier-Augen-Prinzip erfordern

5.2.3 Identifizierung und Authentifizierung der Rollen

Die Identifizierung und Authentifizierung der Rollen erfolgt auf Grundlage des in Abschnitt 5.2.1 und Abschnitt 5.2.2 beschriebenen Rollenmodells. Der technische Zugang zu den IT-Systemen wird durch Nutzerkennung und Passwort oder ein stärkeres Verfahren realisiert. Der physikalische Zugang zu den IT-Systemen wird durch Zutrittskontrollmaßnahmen reglementiert.

5.2.4 Trennung von Rollen

In Tabelle 3 ist aufgeführt, welche Rollen miteinander unverträglich sind.

Rolle	Unverträglich mit				
	TS	CAO1	CAO2	R	ISO
TS - Teilnehmerservice-Mitarbeitende				X	X
CAO1 - CA Mitarbeitende			X	X	X
CAO2 - Systemadministrator/-in		X		X	X
R - Revisor/-in	X	X	X		
ISO - Sicherheitsbeauftragte/-r	X	X	X		

Tabelle 3: Unverträglichkeit von Rollen

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an die Mitarbeitenden

Die Mitarbeitenden der DFN-PCA werden von der Geschäftsführung benannt und eingesetzt. Sie erfüllen alle notwendigen Anforderungen an Vertrauenswürdigkeit, Integrität, Zuverlässigkeit und Fachkunde.

5.3.2 Sicherheitsüberprüfung der Mitarbeitenden

Von allen Mitarbeitenden der DFN-PCA liegt ein regelmäßig zu erneuerndes Führungszeugnis vor.

5.3.3 Anforderungen an die Schulung

In der DFN-PCA werden ausschließlich qualifizierte Mitarbeitende eingesetzt, für die regelmäßig geeignete Schulungen durchgeführt werden. Mitarbeitende erhalten erst nach Nachweis der notwendigen Fachkunde die Berechtigung, spezifische Rollen auszuführen.

5.3.4 Frequenz von Schulungen

Die Frequenz der Schulungen orientiert sich an den Anforderungen der DFN-PCA. Schulungen werden darüber hinaus nach der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

5.3.5 Ablauf und Sequenz der Job Rotation

Es gibt keine Vorgaben für regelmäßige Job Rotation.

5.3.6 Sanktionen für unautorisierte Handlungen

Unautorisierte Handlungen, die die Sicherheit der IT-Systeme der DFN-PCA gefährden oder gegen Datenschutzbestimmungen verstoßen, werden disziplinarisch geahndet und die Arbeitskraft wird ggf. von den betreffenden Funktionen entbunden.

Teilnehmerservice-Mitarbeitende, die gegen ihre Pflichten verstoßen, werden nachgeschult. Bei wiederholtem Verstoß werden sie von ihrer Rolle entbunden und das entsprechende Zertifikat gesperrt.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Keine Angaben.

5.3.8 Dokumente für die Mitarbeitenden

Den Mitarbeitenden der DFN-PCA steht neben diesem CPS das Sicherheitskonzept und die notwendige Betriebsdokumentation zur Verfügung.

5.4 Sicherheitsüberwachung

5.4.1 Überwachte Ereignisse

Zur Abwehr von Angriffen und zur Kontrolle der ordnungsgemäßen Funktion der DFN-PCA werden u. a. nachfolgende Ereignisse mit Zeitpunkt des Auftretens erfasst:

- Fehlgeschlagene Login-Versuche
- Eingang und Genehmigung von Zertifikatanträgen und Sperranträgen (Registrierungsdaten und -Events)
- Ausstellung und Sperrung von Zertifikaten
- Einrichtung und Änderung von Rollenzuordnungen und Berechtigungen
- Erzeugung und Sperrung von CA-Zertifikaten
- Erzeugung, Speicherung, Backup, Wiederherstellung und Vernichtung von privaten Schlüsseln von CA-Zertifikaten
- Betreten und Verlassen der Sicherheitsbereiche
- Verfügbarkeit und Auslastung von Diensten und Netzwerken

5.4.2 Frequenz der Protokollanalyse

Eine Überprüfung der Protokolldaten findet kontinuierlich statt.

5.4.3 Aufbewahrungszeitraum für Protokolldaten

Protokolldaten werden frühestens 1 Jahr nach Ablauf aller mit dem Protokoll in Beziehung stehenden Zertifikate gelöscht.

5.4.4 Schutz der Protokolldaten

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

5.4.5 Backup der Protokolldaten

Die Protokolldaten werden zusammen mit anderen relevanten Daten der DFN-PCA einem regelmäßigen Backup unterzogen.

5.4.6 Überwachungssystem

Es wird ein internes Überwachungssystem verwendet.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Bei schwerwiegenden Ereignissen wird unverzüglich die Rolle ISO informiert. In Zusammenarbeit mit der Rolle CAO2 werden notwendige Aktionen festgelegt, um auf die Ereignisse adäquat reagieren zu können, ggf. wird die Geschäftsführung informiert.

5.4.8 Schwachstellenuntersuchung

Alle drei Monate oder nach größeren Systemänderungen wird ein Vulnerability Scan auf die technischen Systeme der DFN-PCA durchgeführt.

5.5 Archivierung

5.5.1 Archivierte Daten

Dokumente und Daten aus Zertifikatanträgen und der Verifikation der darin enthaltenen Angaben, ausgestellte Zertifikate und Sperrinformationen zu Zertifikaten werden archiviert.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Die in 5.5.1 spezifizierten Daten werden nach Ablauf aller auf diesen Daten basierender Zertifikate mindestens ein Jahr aufbewahrt.

5.5.3 Schutz der Archive

Es wird durch geeignete Maßnahmen sichergestellt, dass die Daten nicht verändert, gelöscht, unbefugt gelesen oder kopiert werden können.

5.5.4 Datensicherungskonzept

Es existiert ein internes Datensicherheitskonzept, nach dem die in Abschnitt 5.4.1 und Abschnitt 5.5.1 aufgeführten Daten gesichert werden.

5.5.5 Anforderungen für Zeitstempel

Die Systemzeit wird mit einer Referenzzeitsynchronisiert.

5.5.6 Archivierungssystem

Es wird ein internes Archivierungssystem verwendet.

5.5.7 Prozeduren zum Abrufen und Überprüfen von archivierten Daten

Die Leitung der DFN-PCA kann den Abruf und die Prüfung der archivierten Daten autorisieren.

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 inkl. Kompromittierung sind dokumentiert und allen Mitarbeitenden zugänglich. Die Prozeduren werden regelmäßig getestet.

5.7.2 Prozeduren bei IT-Systemen

Es existieren Prozeduren zur Wiederherstellung von allen IT-Systemen. Die Prozeduren werden regelmäßig getestet.

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. Zertifikatinhabenden informiert werden.

5.7.4 Betrieb nach einer Katastrophe

Die Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe ist Bestandteil der Notfallplanung.

5.8 Einstellung des Betriebs

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

- Information des Teilnehmers bzw. der Zertifikatinhabenden sowie der Zertifikatprüfende
- Sperrung aller von der CA ausgestellten Zertifikate, somit auch aller Zertifikate von Teilnehmerservice-Mitarbeitern
- sichere Zerstörung der privaten Schlüssel der CA

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

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Die Schlüsselpaare aller CAs werden in einem Hardware-Sicherheitsmodul (HSM), das den Anforderungen aus Abschnitt 6.2.1 genügt, im Vier-Augen-Prinzip erzeugt (siehe Abschnitt 5.2.2).

Teilnehmer erzeugen ihre Schlüssel selbst.

6.1.2 Übermittlung des privaten Schlüssels an den Teilnehmer

Entfällt.

6.1.3 Übermittlung des öffentlichen Schlüssels an den Zertifikatausssteller

Der Certificate Signing Request (CSR) des Teilnehmers wird per HTTPS geschützt 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 4096 Bit haben.

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 oder RSA-PSS signiert.

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.

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 140-2 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 antei-

lig zur Hälfte den Rollen CAO1 und CAO2 bekannt ist.

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-Verein Community-PKI ausgestellten Zertifikate haben folgende Gültigkeitsdauer:

- Zertifikate für CAs: maximal 7300 Tage (ca. 20 Jahre)
- Zertifikate für Datenverarbeitungssysteme: maximal 1170 Tage (ca. 39 Monate)
- Zertifikate für natürliche Personen und Gruppen: maximal 1825 Tage (ca. 5 Jahre)
- Zertifikate können nicht länger gültig sein als das ausstellende CA-Zertifikat.

Für die Gültigkeitsdauer von Schlüsselpaaren gibt es keine Vorgaben.

6.4 Aktivierungsdaten

6.4.1 Aktivierungsdaten für Erzeugung und Installation

Keine Angaben.

6.4.2 Schutz der Aktivierungsdaten

Keine Angaben.

6.4.3 Weitere Aspekte

Keine Angaben.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

Die technischen Systeme, auf denen die DFN-Verein Community-PKI betrieben wird, sind in das Informationssicherheitsmanagement eingebunden. Es werden technische Sicherheits-

maßnahmen im Einklang mit den festgestellten Schutzbedarfen umgesetzt. Insbesondere gilt:

- Die Trennung von Rollen nach Abschnitt 5.2.4 wird von den technischen Systemen unterstützt.
- Netzwerk-Logins sind nur mit Mehrfaktor-Authentifizierung möglich.
- Es gibt eine regelmäßige Integritätsprüfungen der eingesetzten Anwendungen und Betriebssysteme.
- Sicherheitsrelevanten Vorgänge werden zentral geloggt.

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

6.6.1 Softwareentwicklung

Die Erstellung von Software erfolgt durch qualifizierte Mitarbeitende in einer gesicherten Entwicklungsumgebung. Der Einsatz von Software auf einem Produktivsystem erfolgt erst nach Abnahme und Freigabe. Weitere Sicherheitsmaßnahmen zur Softwareentwicklung sind im Sicherheitskonzept enthalten.

6.6.2 Sicherheitsmanagement

Das Sicherheitsmanagement für die DFN-Verein Community-PKI umfasst folgende Aspekte:

- Einbindung in das Informationssicherheitsmanagement
- Überprüfung der Sicherheit im laufenden Betrieb
- Unverzügliche Bewertung von Schwachstellenmeldungen und Auslösung einer der Gefährdung angepassten Reaktion
- Kontinuierliche Einbindung des DFN-CERT

Änderungen an Systemen oder Konfigurationen erfolgen sowohl für reguläre Veränderungen als auch für Notfall-Maßnahmen im Rahmen von Change Control Prozeduren. Diese Änderungen werden dokumentiert.

6.6.3 Lebenszyklus Sicherheitsmaßnahmen

Hardware und Software der CA Systeme werden kontinuierlich gewartet. Lebenszyklus-Controls von Systemen, für die Standardvorgaben existieren, werden eingehalten (siehe z.B. die Regelungen für kryptographische Module nach Abschnitt 6.2.1).

6.7 Sicherheitsmaßnahmen für das Netzwerk

Das Netzwerk der DFN-PCA ist in verschiedene Sicherheitszonen unterteilt, die jeweils durch Firewall-Systeme voneinander getrennt sind. Es gibt ein separates Netzwerk zur Administration. Die Systeme, mit denen die Implementierung der Sicherheitsmaßnahmen administriert werden, werden nicht für andere Zwecke verwendet.

6.8 Zeitstempel

Keine Angaben.

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 nach X.509v3 ausgestellt. Alle Zertifikate enthalten folgende Inhalte:

- Identifizierung der ausstellenden CA
- Der Name des Zertifikatinhabenden oder ein entsprechendes Pseudonym

- Der öffentliche Schlüssel, der mit dem privaten Schlüssel unter der Kontrolle des Zertifikatinhabenden 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/in 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.

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

7.1.5 Namensbeschränkungen

Es wird keine Erweiterung nameConstraints verwendet.

7.1.6 Objekt Identifikator des CPS in Zertifikaten

Die folgenden OIDs werden in alle End-Entity-Zertifikate aufgenommen:

1.3.6.1.4.1.22177.300.2.1.7: Kennzeichnung der CPS DFN-Verein Community-PKI

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkung

Keine Angaben.

7.1.8 Syntax und Bedeutung von Richtlinienkennungen

Siehe Abschnitt 1.2.

7.1.9 Abarbeitung von kritischen Erweiterungen der CP

Keine Angaben.

7.2 CRL Profil

Für jede CA in der DFN-Verein Community-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
- Spätester Zeitpunkt des nächsten Updates im Feld nextUpdate
- Seriennummern und Sperrungsdaten der gesperrten Zertifikate
- Die elektronische Signatur der ausstellenden CA

7.2.1 Versionsnummer

Sperrlisten werden nach X.509 in der Version 2 erstellt.

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 Konformität des Betriebs der PKI zu den Vorgaben dieses CPS und des Sicherheitskonzeptes wird mit internen Audits überprüft. Die Audits werden durch das Informationssicherheitsmanagement gesteuert.

8.1 Frequenz und Umstände der Überprüfung

Als Bestandteil des Informationssicherheitsmanagements wird ein jährliches Audit durchgeführt.

8.2 Identität des Überprüfenden

Audits werden im Regelfall durch Mitarbeitende der DFN-CERT Services GmbH durchgeführt.

8.3 Verhältnis von Prüfenden zu Überprüftem

Prüfende haben keine Rolle CAO1, CAO2 oder TS inne (siehe Abschnitt 5.2.1).

8.4 Überprüfte Bereiche

Es wird der Betrieb der DFN-PKI bei der DFN-PCA überprüft.

8.5 Mängelbeseitigung

Aufgedeckte Mängel werden in einem dem Risiko angemessenen Zeitrahmen behoben.

8.6 Veröffentlichung der Ergebnisse

Ergebnisse werden im Regelfall nicht veröffentlicht.

9 Rahmenvorschriften

9.1 Gebühren

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

9.2 Finanzielle Verantwortung

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

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

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

9.3.2 Nicht vertraulich zu behandelnde Daten

Alle Informationen, die in den 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.

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 der Datenschutzgrundverordnung (DSGVO).

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 gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung

Der DFN-Verein unterliegt dem Recht der Bundesrepublik Deutschland und legt vertrauliche und personenbezogene Daten nur im Einklang mit den geltenden Gesetzen offen.

9.4.7 Andere Umstände einer Veröffentlichung

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

9.5 Urheberrechte

Der DFN-Verein ist Urheber dieses CPS.

9.6 Verpflichtungen

9.6.1 Verpflichtung der Zertifizierungsstellen

Die DFN-Verein Community-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.

9.6.2 Verpflichtung der Registrierungsstellen

Die DFN-PCA verpflichtet sich, alle in diesem CPS beschriebenen Aufgaben durchzuführen.

9.6.3 Verpflichtung des Teilnehmers

Jeder Teilnehmer muss eine Vereinbarung zur Nutzung der DFN-Verein Community-PKI mit dem DFN-Verein unterzeichnen. In dieser verpflichtet sich der Teilnehmer insbesondere zum Einhalten dieses CPS.

9.6.4 Verpflichtung des Zertifikatprüfenden

Es gelten die Bestimmungen aus Abschnitt 4.5.2.

9.6.5 Verpflichtung anderer Beteilige

Sofern weitere Beteiligte als Dienstleister in den Zertifizierungsprozess eingebunden werden, ist die DFN-PCA in der Verantwortung, den Dienstleister zur Einhaltung des CPS der DFN-Verein Community-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

Dieses CPS tritt an dem angegebenen Datum in Kraft. Es wird über den entsprechenden Informationsdienst (siehe Kapitel 2) veröffentlicht.

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-Verein Community-PKI eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Von einer Aufhebung 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 CPS festgelegten Benachrichtigungen bleiben der DFN-PCA freigestellt.

9.12 Änderungen des Dokuments

Die Genehmigung von Änderungen dieses CPS erfolgt durch die Leitung der DFN-PCA.

9.13 Konfliktbeilegung

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

9.14 Geltendes Recht

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

9.15 Konformität mit dem geltenden Recht

Der DFN-Verein sichert zu, geltendes Recht einzuhalten.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Alle in diesem CPS 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 CPS erwachsen, können im Rahmen der üblichen gesetzlichen Vorgaben übertragen werden.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses CPS unwirksam sein oder Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.

Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung weitgehend entspricht. Im Falle von Lücken gilt dasjenige als vereinbart, was nach Sinn und Zweck dieses 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-Verein Community-PKI operierenden CA herrühren, unterliegen 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

Keine Angabe.

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

[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

[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)

[REFEDS_RAF] REFEDS Assurance Framework ver 1.0, https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0

[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

[TCS] GÉANT TCS - Trusted Certificate Service, https://www.geant.org/Services/Trust_identity_and_security/Pages/TCS.aspx

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

11 Glossar

Begriff	Erläuterung
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)

Begriff	Erläuterung
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)
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)
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
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.
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
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

Begriff	Erläuterung
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)
Registrierungsstelle (RA)	Eine Registrierungsstelle (engl.: Registration Authority) registrieren Teilnehmer einer CA und nehmen Zertifikatanträge 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)
Teilnehmerservice	Der Teilnehmerservice übernimmt in Zusammenhang mit der Ausstellung von Zertifikaten Aufgaben, die sinnvollerweise nur lokal beim Teilnehmer durchgeführt werden können.
Teilnehmerservice-Mitarbeitende	Teilnehmerservice-Mitarbeitende beantragen Zertifikate für den Teilnehmer. Darüber hinaus beraten sie Zertifikatinhaber/in und können 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.
Zertifikatinhaber/in	Durch das Subject-Feld des Zertifikats beschriebene Entität, also eine natürliche Person, eine Personengruppe oder ein Datenverarbeitungssystem (engl.: Subject)
Zertifikatname	Synonym: Subject-DN, Name
Zertifikatprüfende	Natürliche oder juristische Personen, die sich auf ein Zertifikat verlassen (engl.: Relying Party)
Zertifizierungsinfrastruktur (PKI)	Bezeichnung für die technischen Einrichtungen sowie die dazugehörenden Prozesse und Konzepte bei der asymmetrischen Kryptographie
Zertifizierungsrichtlinie (CP)	Die Zertifizierungsrichtlinie einer PKI gibt die Regeln vor, an die sich alle Beteiligte halten müssen. In jeder PKI gibt es genau eine Zertifizierungsrichtlinie.
Zertifizierungsstelle (CA)	Wichtigste Aufgabe von Zertifizierungsstellen ist die Ausstellung von Zertifikaten

12 Änderungsverzeichnis

Version	Änderung	Datum
1	Erste Version	15.03.2022
2	1.1: Klarstellung zur Ausrichtung der PKI 3.1.1 und 3.1.2: Zertifikate für Datenverarbeitungssystemen können auch ohne CN ausgestellt werden.	22.06.2026