**Aufgaben des Teilnehmerservice (TS)
in der DFN-PKI
im Sicherheitsniveau Global**

DFN-PKI

1 Ziel des Dokuments

Dieses Dokument fasst die Aufgaben des Teilnehmerservice (TS) einer an der DFN-PKI teilnehmenden Einrichtung (Teilnehmer) zusammen und kann als „kompakter Leitfaden" für Teilnehmerservice-Mitarbeiter verwendet werden.

- In Kapitel 2 werden die Aufgaben des Teilnehmerservice im Überblick dargestellt.
- Kapitel 3 beschreibt die Schritte, die beim Einrichten und Betrieb eines Teilnehmerservice zu beachten sind.
- In Kapitel 4 werden die Arbeitsschritte dargestellt, die von einem TS-Mitarbeiter beim Bearbeiten eines Zertifikatantrags durchzuführen sind.
- Diese Schritte werden in Kapitel 5 in einer Checkliste kurz zusammengefasst.

Die in diesem Dokument zusammengefassten Regelungen und Pflichten ergeben sich aus der Policy der DFN-PKI [CP], zu deren Einhaltung sich jeder Teilnehmer schriftlich verpflichtet hat. Referenzen auf diese Dokumente sind an den entsprechenden Stellen in eckigen Klammern angegeben.

Nur wenn alle Pflichten korrekt wahrgenommen werden, kann ein policy-konformer Betrieb der gesamten DFN-PKI sichergestellt werden. Alle Zertifikate müssen gemäß der zugrunde liegenden Policy ausgestellt werden.

Das bedeutet insbesondere, dass es in der DFN-PKI Global keine „Testzertifikate" gibt und dass das Ausstellen von Zertifikaten mit „Phantasienamen" nicht erlaubt ist. Dies gilt sowohl für Nutzer- als auch für Serverzertifikate.

2 Aufgaben des Teilnehmerservice (TS)

Der Teilnehmerservice eines Teilnehmers übernimmt in Zusammenhang mit der Ausstellung von Zertifikaten Aufgaben, die sinnvollerweise nur lokal durchgeführt werden können.

Die drei wesentlichen Aufgaben sind in den nachfolgenden Unterkapiteln ausgeführt.

2.1 Bearbeiten von Zertifikatanträgen

Die Bearbeitung von Zertifikatanträgen umfasst organisatorische Aufgaben wie beispielsweise die Prüfung, ob eine Person berechtigt ist, ein bestimmtes Zertifikat zu beantragen sowie die persönliche Identifizierung von natürlichen Personen (Zertifikatinhaber). Nach der positiven Prüfung aller Daten erfolgt die Weitergabe des Zertifikatantrags über die elektronische Schnittstelle der Registrierungsstelle (RA-Schnittstelle, Kapitel 3.4) der DFN-PKI. Abschließend müssen anfallende Unterlagen, z. B. der Zertifikatantrag, archiviert werden.

Für eine Zertifikatverlängerung bzw. -erneuerung müssen grundsätzlich dieselben Schritte durchgeführt werden wie bei einer Erstausstellung

Eine detaillierte Zusammenstellung dieser Arbeiten erfolgt in Kapitel 4.

2.2 Sperren von Zertifikaten

Unter bestimmten Bedingungen müssen Zertifikate vom Teilnehmerservice gesperrt werden, z. B. wenn der private Schlüssel eines Zertifikats kompromittiert wurde oder wenn ein Zertifikatinhaber nicht mehr berechtigt ist, ein Zertifikat zu besitzen (z. B. durch Ausscheiden aus der Einrichtung). In diesen Fällen kann entweder durch den Zertifikatinhaber oder durch den Teilnehmerservice ein Sperrantrag ausgelöst werden.

Liegt dem Teilnehmerservice ein Sperrantrag eines Zertifikatinhabers vor, so wird der Teilnehmerservice darüber kurzfristig per E-Mail informiert. Der Teilnehmerservice muss den Sperrantrag dann umgehend über die RA-Schnittstelle bearbeiten.

2.3 Beratung von Nutzern

Jeder Teilnehmerservice sollte seinen Nutzern (Zertifikatinhaber, Server-Administratoren, etc.) Beratung im Umgang mit Zertifikaten anbieten. Dies umfasst die Unterstützung bei der Beantragung von Zertifikaten sowie die technische Unterstützung beim Einsatz von Zertifikaten und bei der Integration der Zertifikate in Anwendungssoftware.

Darüber hinaus muss der Teilnehmerservice seinen Zertifikatinhabern die „Informationen für Zertifikatinhaber" [IfZ] zur Kenntnis bringen.

Die Beratungsfunktion kann außerhalb des Teilnehmerservice auch durch eine andere Stelle wahrgenommen werden, z. B. durch das Rechenzentrum (falls der Teilnehmerservice nicht dort angesiedelt ist) oder die zentrale Nutzerberatung.

3 Einrichten eines Teilnehmerservice

Jede Einrichtung, die an der DFN-PKI teilnimmt (Teilnehmer), benennt zunächst eine handlungsberechtigte Person (HP), die die Einrichtung in allen Belangen im Zusammenhang mit der DFN-PKI gegenüber dem DFN-Verein vertritt. Die HP ist gegenüber dem DFN-Verein für die Einhaltung der Vorgaben gemäß „Pflichten der Teilnehmer der DFN-PKI im Sicherheitsniveau Global" [PdT] in ihrer Einrichtung verantwortlich. Jeder Teilnehmer sollte nach Möglichkeit mehrere handlungsberechtigte Personen benennen, damit auch im Krankheits- oder Urlaubsfall TS-Mitarbeiter eingesetzt und TS-Operator-Zertifikate ausgestellt werden können.

Grundsätzlich veranlasst die HP das Einrichten des Teilnehmerservice, was typischerweise in mehreren Schritten verläuft, die in den folgenden Unterkapiteln dargestellt sind.

3.1 Benennen der Teilnehmerservice-Mitarbeiter

Teilnehmerservice-Mitarbeiter nehmen die täglichen Aufgaben des Teilnehmerservice wahr (s. Kapitel 2). Welche Personen einer Einrichtung mit den Aufgaben des Teilnehmerservice betraut werden, wird in den Einrichtungen selbst bestimmt. Ein TS-Mitarbeiter kann -muss aber nicht- auch handlungsberechtigte Person sein.

Jeder Teilnehmerservice sollte nach Möglichkeit mehrere TS-Mitarbeiter haben, damit auch im Krankheits- oder Urlaubsfall Zertifikat- und Sperranträge ohne Verzögerung erstellt und freigegeben werden können.

Benennungen und Ausscheiden von TS-Mitarbeitern müssen von der handlungsberechtigten Person schriftlich dokumentiert werden. Hierzu gibt es das Formular „F-TS-MA", mit dem TS-Mitarbeiter verpflichtet werden, ihre Aufgaben entsprechend der Vorgaben des Dokuments „Pflichten der Teilnehmer" [PdT] und der Policy [CP] der DFN-PKI durchzuführen. Insbesondere werden sie über die Bedeutung des TS-Zertifikats (s. Kapitel 3.3) unterrichtet und zu einem verantwortungsvollen Umgang mit diesem verpflichtet. Das ausgefüllte Formular wird an die DFN-PCA geschickt, da die DFN-PCA eine Liste aller TS-Mitarbeiter führt. [CP 1.3.2]

TS-Mitarbeiter, die persönliche Identifizierungen auch per Video-Chat vornehmen, müssen eine spezielle Selbstschulung durchführen und diese mit dem Formular „F-TS-Videoschulung" dokumentieren, nachdem sie die „Richtlinie für Video-Identifizierungen in der DFN-PKI" [RVID] und das zugehörige Schulungsvideo zur Kenntnis genommen wurden. Das Formular „F-TS-Videoschulung" verbleibt bei der handlungsberechtigten Person des Teilnehmers. [VID]

3.2 Schaffung der räumlichen und technischen Voraussetzungen

Der Teilnehmerservice sollte in einem nicht öffentlich zugänglichen Raum angesiedelt sein. Zudem muss es einen abschließbaren Schrank (ein normaler Büro-/Aktenschrank ist ausreichend) für Papierunterlagen geben. [CP 4.1.2]

Um die RA-Schnittstelle (s. Kapitel 3.4) zu bedienen, ist ein normaler PC mit einer Java-Laufzeitumgebung (JDK/JRE, ab Version 11) und Internet-Anbindung erforderlich. Es muss die Java RA-Oberfläche für den Teilnehmerservice verwendet werden.

3.3 Bezug eines Teilnehmerservice-Zertifikats

Mit dem Teilnehmerservice-Zertifikat haben TS-Mitarbeiter Zugriff auf die RA-Schnittstelle (s. Kapitel 3.4) und weisen sich somit individuell gegenüber der CA aus. Auf diese Weise werden z. B. Zertifikat- und Sperranträge gesichert vom Teilnehmerservice an die CA weitergeleitet. Hiermit wird bestätigt, dass

- der TS-Mitarbeiter ein Zertifikat für den Zertifikatinhaber/Teilnehmer beantragt;

- der zukünftige Zertifikatinhaber berechtigt ist, das Zertifikat zu bekommen; und
- im Falle von Zertifikaten für eine natürliche Person die persönliche Identifizierung durchgeführt wurde.

Aufgrund der sicherheitskritischen Bedeutung des TS-Zertifikats muss dieses unbedingt vor unberechtigtem Zugriff geschützt werden! Insbesondere muss für das Passwort zur Aktivierung des privaten Schlüssels eine nicht triviale Kombinationen aus mindestens 8 alphanumerischen Zeichen und Sonderzeichen gewählt werden. Anträge für die persönlichen TS-Zertifikate der TS-Mitarbeiter (auch bei Zertifikaterneuerungen im Zuge von Ablauf, Sperrung, etc.) werden immer über die HP der Einrichtung an die DFN-PCA weitergeleitet. Wird ein Mitarbeiter erstmals als TS-Mitarbeiter eingesetzt, so ist ein vom Mitarbeiter und der handlungsberechtigten Person unterschriebenes Formular „F-TS-MA" beizulegen. Die HP übernimmt hierbei auch die persönliche Identifizierung des künftigen TS-Mitarbeiters, falls diese nicht schon anderweitig bei der DFN-PCA vorliegt.

Zertifikate für Teilnehmerservice-Mitarbeiter müssen über die Antragsseiten der für seine Einrichtung betriebenen CA beantragt werden. Hierbei ist der Name in der folgenden Form zu wählen:

"PN: <Vorname Nachname> - Teilnehmerservice <optionales Kürzel>"

3.4 Verwendung der RA-Schnittstelle

Um seine Aufgaben durchführen zu können, wird jedem TS-Mitarbeiter durch den DFN-Verein der Zugang zur grafischen Java-basierten RA-Schnittstelle gewährt, über die sich alle Aufgaben des Teilnehmerservice durchführen lassen.

3.5 Regelmäßige Überprüfung und Schulung

Die HP muss einmal im Jahr überprüfen, dass die Liste der TS-Mitarbeiter des Teilnehmers noch aktuell ist. Hierdurch soll verhindert werden, dass versehentlich noch nicht bei der DFN-PCA abgemeldete ausgeschiedene TS-Mitarbeiter nach wie vor Zugriff haben.

Teilnehmerservice-Mitarbeiter müssen sich regelmäßig über den aktuellen Stand der Dokumente der DFN-PKI informieren, und gegebenenfalls ihre Arbeitsweise anpassen. Diese Selbstschulung soll mindestens einmal im Jahr stattfinden, und muss von der HP dokumentiert werden.

Zur Unterstützung dieser beiden regelmäßig durchzuführenden Tätigkeiten kann in der Java RA-Oberfläche ein Schulungsbogen erstellt werden, der von der HP ausgefüllt und archiviert werden muss. Der Schulungsbogen kann über die Java RA-Oberfläche erstellt werden, indem in der Baumansicht der CA der Punkt „Administration->Teilnehmerservice-Mitarbeiter" gewählt und dann der Kontextmenüeintrag (Rechtsklick) „TS-Schulungsnachweis erstellen" verwendet wird.

3.6 Ausscheiden von Teilnehmerservice-Mitarbeitern

Scheidet ein Teilnehmerservice-Mitarbeiter aus, so muss die HP das Ausscheiden der DFN-PCA mitteilen und das zugehörige TS-Zertifikat sperren.

Für diese Schritte kann die Java RA-Oberfläche benutzt werden, indem in der Baumansicht der CA der Punkt „Administration->Teilnehmerservice-Mitarbeiter" gewählt und dann der Kontextmenüeintrag „TS-Mitarbeiter abmelden" verwendet wird. Hierdurch wird das TS-Zertifikat gesperrt und ein Formular angezeigt, das an die DFN-PCA gesendet werden muss.

4 Arbeitsschritte beim Bearbeiten von Zertifikatanträgen

Reicht ein Antragsteller des Teilnehmers sein Antragsformular beim Teilnehmerservice ein, sind von einem TS-Mitarbeiter mehrere Schritte durchzuführen, bevor der Antrag freigegeben werden kann. [CP 4.1.2]

Die fünf durchzuführenden Arbeitsschritte beim Bearbeiten eines Zertifikatantrags (egal ob Erstantrag oder Verlängerung) sind in den nachfolgenden Unterkapiteln beschrieben.

4.1 Prüfung der Berechtigung des Zertifikatinhabers

Der Teilnehmerservice muss prüfen, ob ein zukünftiger Zertifikatinhaber berechtigt ist, vom Teilnehmer mit einem Zertifikat ausgestattet zu werden.

- Typischerweise können Zertifikate vom Teilnehmer für alle Personen und Datenverarbeitungssysteme im Organisationsbereich des Teilnehmers beantragt werden. Dritte, die nicht unter diese Regelung fallen, können über den Teilnehmerservice keine Zertifikate beantragen. Eine Prüfung kann z. B. anhand von Studierenden- oder Mitarbeiterausweisen erfolgen. [CP 1.3.3]
- Bei Serverzertifikaten ist zu prüfen, ob das Einsatzziel kompatibel mit der DFN-Satzung ist. Insbesondere ist zu beachten, dass das Zertifikat nicht für kommerzielle Zwecke verwendet werden darf. [CP 1.3.3]
- Der Zertifikatinhaber muss der auf dem Zertifikatantrag enthaltenen Einwilligung zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten zugestimmt haben. Dies geschieht durch die Unterschrift unter dem Antrag. Sollte die Einwilligung gestrichen sein, darf kein Zertifikat ausgestellt werden und der Zertifikatantrag (Papier) muss vernichtet werden. Um auch die bei der Erstellung des Antrags erhobenen elektronischen Daten zu löschen, muss der Antrag vom TS-Mitarbeiter in der Java RA-Oberfläche gelöscht werden und eine entsprechende E-Mail an dfnpca@dfn-cert.de geschickt werden, damit alle Datensätze gelöscht werden können.

4.2 Identifizierung des Zertifikatinhabers

Auf jedem Zertifikatantrag gibt es einen Formularbereich, der vom Teilnehmerservice-Mitarbeiter ausgefüllt werden muss. In diesem Bereich wird bei Nutzerzertifikaten die persönliche Identifizierung des Zertifikatinhabers anhand eines „amtlichen Ausweispapiers mit Lichtbild" dokumentiert. Dies umfasst die Prüfung folgender Daten: Name, Unterschrift, Bild, Gültigkeit, Ausweisnummer. [CP 3.2.3]

Während einer Identifizierung muss ein Teilnehmerservice-Mitarbeiter auf Echtheitsmerkmale des vorgelegten Ausweispapiers achten, und offensichtliche Fälschungen ablehnen.

Hinweise zur Prüfung von Ausweisdokumenten, auch ausländischen, finden sich auf der folgenden Web-Seite: https://www.consilium.europa.eu/prado/de.

Wird statt des persönlichen Treffens die Identifizierung per Video-Chat vorgenommen, sind einige Besonderheiten zu beachten. Es ist davon auszugehen, dass ge- oder verfälschte Ausweisdokumente bei einer Begutachtung über Video-Chat schwieriger zu entdecken sind als bei einem persönlichen Treffen. Daher gibt es besondere Anforderungen an die Prüfung des Ausweisdokuments, die im Detail in der Richtlinie für Video-Identifizierung [RVID] beschrieben sind:

- Der die Video-Identifizierung durchführende TS-Mitarbeiter muss die Selbstschulung für die Video-Identifizierung durchlaufen und im Formular „F-TS-Videoschulung" dokumentiert haben.
- Die Identifizierung per Video-Chat ist ausschließlich mit vom DFN dafür freigegeben Ausweisdokumenten, wie sie im Dokument „Merkmale von Ausweisdokumenten" [MvA] aufgeführt sind erlaubt.
- Der TS-Mitarbeiter muss sich bereits vor der eigentlichen Video-Identifizierung mit den Sicherheitsmerkmalen des erwarteten Ausweisdokuments vertraut gemacht haben.
- Für jeden Identifizierungsvorgang per Video-Chat muss die „Checkliste für Video-Identifizierung" [VCL] vom TS-Mitarbeiter ausgefüllt und zusammen mit dem zugehörigen Zertifikatantrag abgelegt werden.

Liegt bei Anträgen für Nutzerzertifikate bereits eine gültige Unterschrift des Zertifikatinhabers beim Teilnehmerservice aus einer früheren Identifizierung vor, die nicht länger als 39 Monate zurückliegt, und hat sich der Name des Zertifikatinhabers nicht geändert, so ist in der Regel keine erneute Prüfung des Ausweises notwendig. Statt dessen kann ein Abgleich mit der vorhandenen Unterschrift auf dem Erstantrag durchgeführt und im Feld „Bereits geprüft" dokumentiert werden.

Bei Serverzertifikaten muss der Antragsteller auch identifiziert werden, um die Berechtigung zum Erhalt des Zertifikats prüfen zu können. Da allerdings keine Verwechslungsgefahr bei Namensgleichheit des Antragstellers besteht, müssen die Daten der Identifizierung nicht in gleichen Umfang wie bei persönlichen Zertifikaten schriftlich dokumentiert werden.

4.3 Prüfung der E-Mail-Adressen in Zertifikaten

Der Teilnehmerservice muss sicherstellen, dass die in das Zertifikat aufzunehmende(n) E-Mail-Adresse(n) dem Teilnehmer bzw. künftigen Zertifikatinhaber zugeordnet sind oder diese vom Besitzer der E-Mail-Adresse autorisiert sind, die E-Mail-Adressen zu nutzen. [CP 3.1.2, 3.2.3]

Stammt die angegebene E-Mail-Adresse aus dem Bereich des Teilnehmers, lässt sich dies grundsätzlich leicht feststellen. Werden stattdessen nicht von der Einrichtung selbst verwaltete E-Mail-Adressen verwendet (z. B. gmx.de, web.de), ist es generell aufwändig, für den Teilnehmerservice zu erkennen, ob sie dem Zertifikatinhaber zugeordnet sind.

Deshalb wird in den technischen Systemen der DFN-PKI eine Liste von zugelassenen Domains für E-Mail-Adressen geführt. Diese E-Mail-Domains kann der Teilnehmerservice über die Java RA-Oberfläche freischalten lassen (in der Baumansicht der CA über „Administration->Konfiguration E-Mail-Domains“). Die Freischaltung erfordert die Zustimmung des Domaininhabers oder technischen Ansprechpartners über ein Challenge-Response-Verfahren per E-Mail. Die Freischaltung ist für 825 Tage gültig. Nach Ablauf muss sie durch den Teilnehmerservice erneut veranlasst werden.

Für E-Mail-Adressen, die aus Domains aus dieser Liste stammen, muss der Teilnehmerservice selbst sicherstellen, dass diese dem Zertifikatinhaber zugeordnet sind. Dies kann beispielsweise durch interne Adresslisten o. ä. geschehen. Sind in einem Zertifikatantrag E-Mail-Adressen enthalten, die **nicht** aus einer Domain aus dieser Liste stammen, so wird an diese E-Mail-Adressen eine E-Mail geschickt, in der ein Bestätigungs-Link enthalten ist. Der Zertifikatantrag kann nicht genehmigt werden, bevor nicht der Bestätigungs-Link aufgerufen wurde. Dem Teilnehmerservice wird durch den Textzusatz „Bestätigt durch Nutzer“ signalisiert, dass der E-Mail-Empfänger den Bestätigungs-Link aufgerufen hat.

Der Teilnehmerservice kann das (erneute) Versenden einer Bestätigungs-E-Mail manuell auslösen.

Auf Wunsch können die technischen Systeme der DFN-PKI auch so konfiguriert werden, dass ausschließlich E-Mail-Adressen aus der Liste der zugelassenen E-Mail-Domains verwendet werden können und keine Bestätigungs-E-Mails verschickt werden.

4.4 Prüfung des DN

Der DN eines Zertifikatinhabers muss eindeutig und aussagekräftig sein und darf nicht an verschiedene Zertifikatinhaber vergeben werden. Generell darf der DN keine Umlaute oder andere Sonderzeichen enthalten. Erlaubte Zeichen in den DN-Attributen ST, L, O, OU und CN sind [CP 3.1.4]:

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

Für die Ersetzung deutscher Sonderzeichen gelten folgende Substitutionsregeln:

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

Jedes Vorkommen von OU im DN muss den Namen einer organisatorischen Untereinheit der im O genannten Organisation enthalten. Insbesondere dürfen keinesfalls Platzhalter wie „.“ und „-“ oder Floskeln wie „Nicht anwendbar“ verwendet werden.

Falls mehrere OU-Attribute 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.

In den folgenden Unterkapiteln sind die Punkte aufgeführt, die je nach Zertifikattyp zusätzlich geprüft werden müssen.

4.4.1 Zertifikate für natürliche Personen (Nutzerzertifikate)

- Der Name im CN-Attribut muss aus mindestens einem ausgeschriebenen Vornamen und dem vollständigen Nachnamen wie im amtlichen Ausweispapier mit Lichtbild bestehen. [CP 3.1.2 b]
- Namenszusätze, die im amtlichen Ausweispapier geführt werden (z. B. „Dr.”), können in den CN-Attribut aufgenommen werden. Darin nicht aufgeführte Namenszusätze (z. B. „Prof.”) dürfen nicht im CN-Attribut verwendet werden. [CP 3.1.2 b]
- Jeder DN muss eindeutig sein und darf nicht an mehrere Zertifikatinhaber vergeben werden. Wenn ein DN durch die gewählte Kombination der Attribute wie z. B. O, OU, L, ST und CN nicht eindeutig wäre, so muss die Eindeutigkeit durch die Verwendung von

zusätzlichen OU, UID oder SER Attributen oder durch die Verwendung von Pseudonymen im Attribut CN wie z. B. „PN: Max Mustermann 2“ sichergestellt werden. Hinweis: Für die Eindeutigkeit reicht es aus, wenn auch nur ein Attribut im DN unterschiedlich ist, also z. B. das OU-Attribut. [CP 3.1.5]

- Gehört der Zertifikatinhaber nicht unmittelbar zum Teilnehmer, so muss dem Namen das Kennzeichen „EXT - ” oder „EXT:” vorangestellt werden, z. B. „CN=EXT:Max Mustermann”. [CP 3.1.2 b]

4.4.1.1 Pseudonyme

- Das CN-Attribut eines Pseudonyms muss mit dem Kennzeichen „PN:” oder „PN - ” beginnen, z. B. „CN=PN:Deckname”. [CP 3.1.2 b]
- Bei der Vergabe von Namen für Pseudonyme muss eine Verwechslung mit existierenden Namen, z. B. mit natürlichen Personen oder Organisationen, ausgeschlossen werden. Ebenso dürfen keine Domain-Namen, IP-Adressen oder andere innerhalb der DFN-PKI benutzte Syntaxelemente („GRP” oder „EXT”) verwendet werden. Ein Pseudonym darf keinen beleidigenden oder anzüglichen Inhalt enthalten. [CP 3.1.2 b]

Das Pseudonym muss dem Zertifikatinhaber eindeutig zugeordnet sein.

4.4.2 Zertifikate für Datenverarbeitungssysteme (Server-Zertifikate)

- Bei Zertifikaten für Datenverarbeitungssysteme (z. B. Server-Zertifikate) muss für den Namen der voll qualifizierte Domain-Name (FQDN) verwendet werden, z. B. „CN=pki.p-ca.dfn.de”. [CP 3.1.2 a]
- Die Ausstellung sogenannter „Wildcard-Zertifikate”, z. B. „CN=*.pca.dfn.de”, ist möglich. Da Wildcard-Zertifikate für eine ganze Subdomain verwendet werden können, ist der potentielle Schaden bei einer Kompromittierung des privaten Schlüssels deutlich höher als bei Zertifikaten für genau spezifizierte FQDNs. Daher sollten Wildcard-Zertifikate in der DFN-PKI nur verwendet werden, wenn das Einsatzszenario dies technisch erzwingt. Beispielsweise gibt es Softwaresysteme, die dynamisch Host-Namen erzeugen (gerade im Bibliotheksumfeld), die mit herkömmlichen Zertifikaten schlicht nicht funktionieren. Beispiele für solche Software: EZProxy, Netman/HAN. Ein und dasselbe Wildcard-Zertifikat sollte nicht auf verschiedenen Servern mit unterschiedlichen Diensten, Einsatzzwecken oder Schutzklassen verwendet werden. Aufgrund des höheren Schadenspotentials bei Kompromittierung sind Wildcard-Zertifikate kein probates Mittel der Arbeitsersparnis bei der Zertifikatbeantragung. Wildcard-Zertifikate sollten daher nur unterhalb von Sub-Domains oder Second-Level-Domains ausgestellt werden, die ausschließlich für einen klar abgegrenzten Zweck genutzt werden, also beispielsweise entweder für "*.roaming.dfn.de" oder für "*.dfnroaming.de", nicht aber für "*.dfn.de".
- Für jeden Teilnehmer wird von der DFN-PCA eine Liste von im FQDN zulässigen Domain-Namen geführt. Es können nur Zertifikate mit FQDNs ausgestellt werden, deren Domain auf dieser Liste steht. Der Teilnehmerservice kann Domains über die Java RA-Oberfläche freischalten lassen (in der Baumansicht der CA über „Administration->Konfiguration Server-Domains“). Die Freischaltung erfordert die Zustimmung des Domaininhabers oder technischen Ansprechpartners über ein Challenge-Response-Verfahren per E-Mail. Die Freischaltung ist für 825 Tage gültig. Nach Ablauf muss sie durch den Teilnehmerservice erneut veranlasst werden. [CP 3.1.2 a, 3.2.2]

4.4.3 Zertifikate für Personengruppen (Gruppenzertifikate)

- Zertifikate für Personengruppen müssen mit dem Kennzeichen „GRP:” oder „GRP - ” beginnen, z. B. „CN=GRP:Poststelle”. [CP 3.1.2 c]
- Bei der Vergabe von Namen für Personengruppen muss eine Verwechslung mit existierenden Namen, z. B. mit natürlichen Personen oder Organisationen, ausgeschlossen werden. Ob Verwechselungsgefahr besteht oder nicht, muss der TS-Mitarbeiter selbst einschätzen. Hierzu kann der TS-Mitarbeiter bereits vergebene Zertifikatsnamen mit ähnlichem oder verwandtem Inhalt, den angestrebten Einsatzzweck, die vorgesehenen Gruppenmitgliedern sowie die vorliegende Organisationsstruktur berücksichtigen. Falls Verwechselungsgefahr besteht, muss ein anderer GRP-Name gewählt werden.
- Es dürfen keine Domain-Namen, IP-Adressen oder andere innerhalb der DFN-PKI benutzte Syntaxelemente („PN” oder „EXT”) verwendet werden. [CP 3.1.2 c]

4.5 Archivierung der Identifizierungsformulare

Alle beim Teilnehmerservice anfallenden Papierunterlagen und elektronischen Dokumente, die die persönliche Identifizierung von Zertifikatinhabern betreffen, müssen archiviert werden, um auch über die Lebensdauer der diesen Zertifikatinhabern zugehörigen Zertifikate hinaus die persönliche Identifizierung belegen zu können. Das beinhaltet bei Identifizierungen per Video-Chat auch die „Checkliste für die Video-Identifizierung“.

Papierunterlagen oder elektronische Dokumente, die persönliche Identifizierungen dokumentieren, müssen für mindestens sieben (7) Jahre nach Ablauf des letzten Zertifikats, das auf Basis dieser Unterlagen ausgestellt wurde, aufbewahrt werden. [CPS der PKI 5.4.3 und 5.5]

5 Checkliste für die Bearbeitung von Zertifikatanträgen

Die folgenden Schritte sind von einem TS-Mitarbeiter durchzuführen, bevor ein Zertifikatantrag durch die Signatur mit dem TS-Zertifikat freigegeben werden darf.

Eine ausführliche Beschreibung der Schritte findet sich in Kapitel 4, die nachfolgende Checkliste fasst die Punkte in Kurzform zusammen und kann der eigenen Kontrolle dienen.

Durchzuführende Schritte:

- ☐ Zertifikatinhaber ist berechtigt, mit einem Zertifikat versorgt zu werden (Organisationsbereich des Teilnehmers) [s. Kapitel 4.1]
- ☐ Identifikation des Zertifikatinhabers (persönliches Zertifikat/Pseudonym) ist auf Formular dokumentiert [s. Kapitel 4.2]
  - ☐ Checkliste für die Video-Identifizierung ist ausgefüllt (nur bei Video-Identifizierung) [s. Kapitel 4.2]
- ☐ E-Mail-Adresse(n) im Zertifikat (DN und alternative Namen) sind dem Zertifikatinhaber oder dem Teilnehmer zugeordnet [s. Kapitel 4.3]
- ☐ Prüfung des DN (keine Sonderzeichen) [s. Kapitel 4.4]
  - ☐ OU ist eine organisatorische Untereinheit des Teilnehmers und keine eigenständige juristische Person [s. Kapitel 4.4]
  - ☐ OU enthält keine Platzhalter wie „.“ oder „Nicht anwendbar“ [s. Kapitel 4.4]
  - ☐ Serverzertifikate -auch alternative Namen- (FQDN, Zustimmung Domaininhaber, IP-Adressen) [s. Kapitel 4.4.2]
  - ☐ Nutzerzertifikate (Name wie Ausweis, Namenszusätze, eindeutig) [s. Kapitel 4.4.1]
  - ☐ Pseudonyme („PN”, keine existierenden Namen/Domains/IP-Adressen, nicht beleidigend/anzüglich, eindeutig) [s. Kapitel 4.4.1.1]
  - ☐ Externer Zertifikatinhaber (nicht unmittelbar zum Teilnehmer gehörende Person, „EXT”, Name wie Ausweis, Namenszusätze, eindeutig) [s. Kapitel 4.4.1]
  - ☐ Personengruppen („GRP”, keine existierenden Namen/Domains/IP-Adressen, Berechtigung) [s. Kapitel 4.4.3]4.5
- ☐ Archivierung der persönlichen Identifizierung, falls zutreffend inkl. der Checkliste für die Video-Identifizierung [s. Kapitel 4.5]

Zusätzlich muss der Teilnehmerservice den Zertifikatinhaber auf die „Informationen für Zertifikatinhaber” [IfZ] hinweisen.

6 Glossar

Begriff	**Erläuterung**
Antragsteller	Antragsteller ist immer ein Teilnehmer (engl.: Applicant)
C	Bestandteil des DN: Staat
CA	Zertifizierungsstelle (engl.: Certification Authority)
CN	Bestandteil des DN: Name (engl.: Common Name)
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)
DN	Eindeutiger Name des Zertifikatinhabers bzw. -ausstellers in Zertifikaten. Ein DN wird aus mehreren Bestandteilen wie z. B. C, ST, L, O, OU, CN gebildet. (engl.: Distinguished Name)
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)
Informationen für Zertifikatinhaber	Informationen zum Umgang mit privaten Schlüsseln für Zertifikatinhaber (engl.: Subject Information)
L	Bestandteil des DN: Ort
O	Bestandteil des DN: Organisation
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)
OU	Bestandteil des DN: Organisationseinheit (engl.: Organizational Unit)
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 (RA)	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
ST	Bestandteil des DN: Bundesland
Teilnehmer	Teilnehmer ist immer eine Organisation, i. d. R. ein DFN-Anwender (engl.: Subscriber)
Teilnehmerservice-Mitarbeiter (TS-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

Begriff	Erläuterung
Zertifikatantrag	Dokument in Papierform oder elektronisch, mit dem bei einer CA die Ausstellung eines Zertifikates beantragt wird. Ein Zertifikatantrag beinhaltet den Namen des Zertifikatinhabers, des Teilnehmers, den gewünschten DN im Zertifikat und grundsätzlich den öffentlichen Schlüssel.
Zertifikatinhaber	Durch das Subject-Feld des Zertifikats beschriebene Entität, also eine natürliche Person, eine Personengruppe oder ein Datenverarbeitungssystem (engl.: Subject)
Zertifikatname	Synonym: Subject-DN, Name
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.

7 Referenzen

[CP] Policies der DFN-PKI, https://www.pki.dfn.de/policies/
[IfZ] Informationen für Zertifikatinhaber in der DFN-PKI im Sicherheitsniveau Global, https://www.pki.dfn.de/fileadmin/PKI/Info_Zertifikatinhaber.pdf
[MvA] Merkmale von Ausweisdokumenten, https://www.pki.dfn.de/fileadmin/PKI/VideoIdent/Merkmale_von_Ausweisdokumenten.pdf
[PdT] Pflichten der Teilnehmer der DFN-PKI im Sicherheitsniveau Global, https://www.pki.dfn.de/fileadmin/PKI/Pflichten-der-Teilnehmer.pdf
[RVID] Richtlinie für die Video-Identifizierung in der DFN-PKI, https://www.pki.dfn.de/fileadmin/PKI/VideoIdent/Richtlinien-Video-Identifizierung-DFN-PKI.pdf
[VCL] Checkliste für die Durchführung einer Video-Identifizierung, https://www.pki.dfn.de/fileadmin/PKI/VideoIdent/F-ID-Video-Checkliste.pdf
[VD] Informationen zur Video-Identifizierung in der DFN-PKI, https://www.pki.dfn.de/policies/videoident/