Pflichten der Teilnehmer der DFN-PKI im Sicherheitsniveau Global

DFN-PKI

1 Einleitung

Dieses Dokument richtet sich an Teilnehmer der DFN-PKI im Sicherheitsniveau Global.

1.1 Teilnehmer

Teilnehmer sind Organisationen, die an der DFN-PKI teilnehmen und eine entsprechende Vereinbarung mit dem DFN-Verein unterzeichnet haben. Dieses Dokument ist Bestandteil dieser Vereinbarung.

Teilnehmer der DFN-PKI beantragen Zertifikate für Personen und Datenverarbeitungssysteme in ihrem Organisationsbereich. Diese Personen und Datenverarbeitungssysteme sind die Zertifikatinhaber.

Jeder Teilnehmer hat Pflichten, die im Folgenden beschrieben werden.

1.2 Teilnehmerservice

Der Teilnehmerservice übernimmt in Zusammenhang mit der Ausstellung von Zertifikaten Aufgaben, die sinnvollerweise nur lokal beim Teilnehmer durchgeführt werden können, z. B. die Beratung und die persönliche Identifizierung der Zertifikatinhaber.

Teilnehmerservice-Mitarbeiter werden gegenüber dem DFN von einer Handlungsberechtigten Person benannt. Die Handlungsberechtigte Person ist darüber hinaus dafür verantwortlich, ausscheidende Teilnehmerservice-Mitarbeiter bei der DFN-PCA unverzüglich abzumelden. Die Abmeldung erfolgt über das entsprechende Formular per Post. Zusätzlich sollte die Abmeldung per E-Mail an die DFN-PCA erfolgen, um die erfolgreiche Abmeldung auch bei Verlust des Formulars auf dem Postweg sicherzustellen.

1.3 Handlungsberechtigte Person

Jeder Teilnehmer benennt eine oder mehrere handlungsberechtigte Personen, die den Teilnehmer in allen Belangen im Zusammenhang mit der DFN-PKI gegenüber dem DFN-Verein vertritt.

Die handlungsberechtigte Person ist gegenüber dem DFN-Verein für die Einhaltung der Pflichten gemäß diesem Dokument in ihrer Einrichtung zuständig.

1.4 Aufbewahrungsfristen

Die in Kapitel 5.5.1 der Erklärung zum Zertifizierungsbetrieb spezifizierten Daten werden nach Ablauf aller auf diesen Daten basierenden Zertifikaten mindestens sieben Jahre aufbewahrt.

1.5 Audit-Schema

Die DFN-PKI erfüllt im Sicherheitsniveau "Global" die Anforderungen von ETSI EN 319 411-1 nach der OVCP-Policy für Zertifikate für Datenverarbeitungssysteme bzw. nach der NCP-Policy für Zertifikate für Personen und die Anforderungen von ETSI EN 319 401.

1.6 Geltendes Recht

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

2 Generelle Pflichten der Teilnehmer

2.1 Einhaltung von CP und CPS

Teilnehmer sind verpflichtet, die Zertifizierungsrichtlinie (CP) und die Erklärung zum Zertifizierungsbetrieb (CPS) der DFN-PKI im Sicherheitsniveau Global einzuhalten. Die beiden Dokumente sind erhältlich unter https://www.pki.dfn.de/policies.

Aus CP und CPS ergeben sich Pflichten, die in den folgenden Abschnitten dargelegt werden.

2.2 Schulung der Teilnehmerservice-Mitarbeiter

Teilnehmerservice-Mitarbeitern werden bei ihrer Ernennung die Policy der DFN-PKI (CP und CPS) sowie die Dokumente „Pflichten der Teilnehmer“, „Aufgaben des Teilnehmerservice in der DFN-PKI“ und „Informationen für Zertifikatinhaber“ zur Kenntnis gegeben. Wenn durch die DFN-PCA neue Versionen dieser Dokumente bekannt gegeben werden, müssen diese ebenfalls allen Teilnehmerservice-Mitarbeitern zur Kenntnis gegeben werden. Die Kenntnisnahme durch die Teilnehmerservice-Mitarbeiter muss dokumentiert werden.

2.3 Wahrheitspflicht

Alle Angaben, die Teilnehmer gegenüber der DFN-PKI machen, müssen korrekt sein.

2.4 Nutzung von Zertifikaten der DFN-PKI

Teilnehmer dürfen Zertifikate der DFN-PKI nur unter Berücksichtigung der Satzung des DFN-Vereins beantragen und verwenden. Die möglichen Einsatzarten ergeben sich insbesondere aus §2 der Satzung:

„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 [...].”

Zertifikate, die entgegen der Satzung des DFN-Vereins beantragt oder verwendet werden, können von der DFN-PCA gesperrt werden.

2.5 Aktualität von Daten

Wechsel bei den handlungsberechtigten Personen (Kap. 1.3) oder im Personal des Teilnehmerservice (Kap. 1.2) müssen dem DFN-Verein vom Teilnehmer mitgeteilt werden.

Änderung des Namens des Teilnehmers oder des Wechsels der Rechtsform müssen dem DFN-Verein ebenfalls angezeigt werden.

2.6 Verwendung von Warenzeichen

Es liegt in der alleinigen Verantwortung des Teilnehmers, dass die Namenswahl in Zertifikaten keine Warenzeichen o. ä. verletzt. Der DFN-Verein ist nicht verpflichtet, solche Rechte zu überprüfen. Falls der DFN-Verein über eine Verletzung solcher Rechte informiert wird, muss das Zertifikat gesperrt werden.

2.7 Audit

Das Sicherheitsniveau „Global“ der DFN-PKI wird zur Aufrechterhaltung der Browserverankerung regelmäßig auditiert. Zur Durchführung dieser Audits müssen die Teilnehmer dem von der DFN-PKI beauftragten Auditor Zugang zum Teilnehmerservice und dessen Unterlagen gewähren. Zur Durchführung dieser Audits ist die Mithilfe der Teilnehmer erforderlich, z.B. durch die Gewährung des Zugangs zum Teilnehmerservice gegenüber dem durch die DFN-PKI beauftragten Auditor.

3 Betrieb des Teilnehmerservice

Wenn vom Teilnehmer ein Teilnehmerservice betrieben wird, müssen die im Dokument „Aufgaben des Teilnehmerservice“ beschriebenen Pflichten eingehalten werden.

Insbesondere bedeutet das:

- Identifizierungen von Zertifikatinhabern müssen korrekt durchgeführt werden. Die mit dem Betrieb des Teilnehmerservice beauftragten Personen werden von jeglichem Einfluss, der die Objektivität und Neutralität des Betriebs des Teilnehmerservice beeinträchtigen könnte, freigehalten.
- Zertifikatinhabern müssen die Regelungen aus dem Dokument „Informationen für Zertifikatinhaber” ausgehändigt bzw. zugänglich gemacht werden.

- Papierunterlagen und elektronische Dokumente müssen für mindestens 7 Jahre nach Ablauf des letzten Zertifikats, das auf Basis dieser Unterlagen ausgestellt wurde, aufbewahrt werden.
- Für Zertifikate ist unverzüglich eine Sperrung einzuleiten, wenn deren Inhalte nicht mehr korrekt sind, die dazugehörigen privaten Schlüssel kompromittiert wurden oder die Berechtigung für die Nutzung des Zertifikats nicht mehr vorliegt.
- Wechsel beim Personal des Teilnehmerservice werden der DFN-PCA unverzüglich angezeigt.

Zum Betrieb des Teilnehmerservice ist ein technischer Zugang erforderlich. Dieser Zugang darf nur auf Systemen genutzt werden, die die folgenden Mindest-Anforderungen an die IT-Sicherheit erfüllen:

- Das System muss angemessen geschützt und professionell betrieben werden.
- Es muss frei von Schadsoftware wie Viren sein.
- Das Betriebssystem muss aktuellen Support haben.
- Es müssen regelmäßig Sicherheits-Patches eingespielt werden.
- Die betriebssystemeigenen Sicherheitsmechanismen müssen nach Möglichkeit aktiviert sein (z.B. Firewall, Virenscanner).
- Der administrative Zugriff ist klar geregelt.

4 Zentrale teilnehmerinterne Schlüsselerzeugung

Wenn im Rahmen der Zertifikatbeantragung Schlüssel von einer anderen Person als dem Zertifikatinhaber erzeugt werden, so ist dies nur unter folgenden Bedingungen gestattet:

- Die Schlüsselerzeugung findet mit Algorithmen statt, die zu qualitativ hochwertigem Schlüsselmaterial führen. Insbesondere werden kryptographisch sichere Zufallszahlengeneratoren mit zufälligen Initialisierungswerten benutzt.
- Die Schlüsselerzeugung wird auf eine Art durchgeführt, die die Verwendung des privaten Schlüssels durch andere Personen als den Zertifikatinhaber wirksam verhindert. Insbesondere wird der Schlüssel stets durch eine PIN oder Passphrase geschützt. Die PIN oder Passphrase muss zufällig erzeugt werden und mindestens 8 Zeichen lang sein.
- Alternativ kann für Crypto-Token und Smartcards mit nicht auslesbaren privaten Schlüsseln ein Verfahren eingesetzt werden, bei dem der Zertifikatinhaber den privaten Schlüssel vor der ersten Nutzung durch Setzen einer PIN/Passphrase freischalten muss und bei dem eine unberechtigte Freischaltung angezeigt wird („Null-PIN Verfahren“).
- Der private Schlüssel muss nach der Übergabe unwiederbringlich von zentralen Teilnehmerservice-Systemen gelöscht werden (Ausnahme: Hinterlegte Schlüssel nach Abschnitt 5).
- Der private Schlüssel und die PIN/Passphrase werden dem Zertifikatinhaber so übergeben, dass niemand anders als ihm PIN/Passphrase und privater Schlüssel bekannt sind.
- Erzeugte Schlüssel, Zertifikate und PIN-Briefe müssen nach der Erstellung nach spätestens 8 Wochen an den Zertifikatinhaber übergeben werden. Die Aufbewahrung muss so geschehen, dass ein unbefugter Zugriff wirksam verhindert wird. Ist eine Übergabe nach 12 Wochen nicht erfolgt, müssen die Schlüssel und PIN-Briefe vernichtet und die Zertifikate gesperrt werden.

5 Zentrale teilnehmerinterne Schlüsselhinterlegung und -wiederherstellung

Wenn beim Teilnehmer ein Verfahren zur internen Schlüsselhinterlegung eingesetzt wird, mit dem private Schlüssel von Zertifikatinhabern wiederhergestellt werden können, so ist dies nur unter folgenden Bedingungen gestattet:

- Die Zertifikatinhaber werden darüber informiert, dass eine Schlüsselhinterlegung stattfindet.

- Die hinterlegten Schlüssel werden verschlüsselt gespeichert.
- Private Schlüssel zu Signaturzertifikaten sollten nicht zentral hinterlegt werden. Eine Hinterlegung untergräbt das Vertrauen in die damit erstellten Signaturen und erfüllt keinen konkreten Zweck, da im Fall des Verlustes eines privaten Signaturschlüssels ein neuer Schlüssel erzeugt und verwendet werden kann.
- Die Wiederherstellung von privaten Schlüsseln erfolgt in der Regel nur für den zugehörigen Zertifikatinhaber. Die Wiederherstellung von privaten Schlüsseln für Personen, die nicht der Zertifikatinhaber sind (im Folgenden „Dritte“ genannt), findet nur statt, wenn es hierfür organisatorische Regelungen und Prozesse gibt, in denen der Datenschutzbeauftragte oder die Geschäftsführung einbezogen sind. Zugehörige Zertifikate sind bei einer Übergabe von privaten Schlüsseln an Dritte sofort zu sperren, neue Zertifikate dürfen nicht auf der Basis dieser Schlüssel erstellt werden.
- Die Wiederherstellung von Schlüsseln wird auf eine Art durchgeführt, die die Verwendung der privaten Schlüssel durch andere Personen als den jeweiligen Zertifikatinhaber oder o. g. Dritte wirksam verhindert. Insbesondere werden Schlüssel stets durch eine PIN oder Passphrase geschützt. Die PIN oder Passphrase muss zufällig erzeugt werden und mindestens 8 Zeichen lang sein.
- Alternativ kann für eine Wiederherstellung auf Crypto-Token und Smartcards mit nicht auslesbaren privaten Schlüsseln ein Verfahren eingesetzt werden, bei dem der Zertifikatinhaber oder o. g. Dritte den privaten Schlüssel vor der ersten Nutzung durch Setzen einer PIN/Passphrase freischalten müssen und bei dem eine unberechtigte Freischaltung angezeigt wird („Null-PIN Verfahren“).
- Kopien des privaten Schlüssels, die im Zuge der Wiederherstellung auf zentralen Teilnehmerservice-Systemen abfallen, müssen nach der Übergabe unwiederbringlich von diesen gelöscht werden.
- Die wiederhergestellten privaten Schlüssel und die PIN/Passphrase werden dem Zertifikatinhaber oder o. g. Dritten so übergeben, dass niemand anders als sie Kenntnis der PIN/Passphrase und des Schlüssels erlangen können.

6 Zentrale Verwendung von Nutzer-Schlüsseln

Wenn beim Teilnehmer ein Verfahren eingesetzt wird, bei dem private Schlüssel von Nutzern auf zentralen Geräten eingesetzt werden (z.B. Mail-Appliances mit Verschlüsselungs-/Signaturfunktion), so ist dies nur unter folgenden Bedingungen gestattet:

- Die Zertifikatinhaber werden darüber informiert, dass ihre Schlüssel auf einem zentralen Gerät abgelegt werden.
- Jedes zentrale Gerät, auf dem private Schlüssel von Nutzern vorgehalten werden, muss angemessen geschützt werden. Das heißt z. B.:
    - Das Gerät befindet sich in einer gesicherten Infrastruktur, z. B. hinter einer geeignet konfigurierten Firewall.
    - Das Gerät wird professionell betrieben, u. a. durch regelmäßiges Einspielen von Sicherheits-Patches.
    - Der administrative Zugriff auf das Gerät ist klar geregelt.
- Die privaten Schlüssel von Nutzern liegen auf dem Gerät nicht im Klartext auf dauerhaften Speichern vor. Es sind Schutzmechanismen gegen eine Kompromittierung der Schlüssel bei einem Einbruch in das Gerät oder dessen physikalischen Diebstahl vorhanden. Die unberechtigte Extraktion der privaten Schlüssel wird verhindert.
- Eine Signatur wird mit den privaten Schlüsseln der Nutzer durch das Gerät nur erstellt, wenn nachweislich ausschließlich der Zertifikatinhaber eine Signaturerstellung angefordert hat. Ein geeigneter Mechanismus ist z.B. für Mail-Appliances eine SMTP-Authentisierung des Zertifikatinhabers vor jeder Signaturerstellung.