Informationen für Zertifikatinhaber in der DFN_Community-PKI

DFN-PKI

1 Einleitung und Hintergrund

Dieses Dokument richtet sich an Personen, die ein Zertifikat in der DFN-Community-PKI beantragt und erhalten haben. Informationen zur DFN-Community-PKI finden Sie unter https://www.pki.dfn.de/dfn-verein-community-pki

In den folgenden Abschnitten wird beschrieben, welche Regelungen und Pflichten Sie als Inhaber eines Zertifikats der DFN-Comunity-PKI - im folgenden Zertifikatinhaber - einhalten müssen. Diese Regelungen und Pflichten ergeben sich aus der Erklärung zum Zertifizierungsbetrieb (CPS) der DFN-Community-PKI, einzusehen unter:
https://www.pki.dfn.de/fileadmin/PKI/DFN-Verein_Community_PKI_CPS.pdf

2 Beantragung und Annahme

Sie sind verpflichtet, bei der Beantragung von Zertifikaten in der DFN-Community-PKI korrekte Daten anzugeben.

Als Zertifikatinhaber sind Sie verpflichtet, innerhalb von 14 Tagen nach Erhalt eines Zertifikats die Korrektheit der enthaltenen Daten zu überprüfen. Sind die enthaltenen Daten nicht korrekt, müssen Sie das Zertifikat wieder sperren lassen.

3 Nutzung von Zertifikaten der DFN-Community-PKI

Sie dürfen Zertifikate der DFN-CommunityPKI nur unter Berücksichtigung der CPS der DFN-Community-PKI) und damit auch der Satzung des DFN-Vereins verwenden. Insbesondere ist Zu beachten, dass ein Zertifikat der DFN-Community-PKI nicht für kommerzielle Zwecke verwendet Werden darf. [CPS1.4 und 1.3.3 mit Verweis auf Satzung des DFN-Vereinn §2 Vereinszweck]

Sie akzeptieren, dass die DFN-PCA das Recht hat, Ihr Zertifikat unverzüglich zu sperren, wenn Sie gegen die hier aufgeführten Regelungen und Pflichten verstoßen oder wenn dies aufgrund einer Anforderung aus der Zertifizierungsrichtlinie oder der Erklärung zum Zertifizierungsbetrieb notwendig ist.

Sie sind verpflichtet, auf Anweisungen der DFN-PCA im Fall von kompromittierten Schlüsseln oder Missbrauch von Zertifikaten zu reagieren.

4 Verpflichtung zur Sperrung

Als Zertifikatinhaber sind Sie unter den folgenden Bedingungen verpflichtet, Ihr Zertifikat sperren zu lassen:

- Das Zertifikat enthält Angaben, die nicht mehr gültig sind, beispielsweise nach einer Namensänderung.
- Der private Schlüssel oder das dazugehörige Passwort/PIN wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Sie sind nicht mehr berechtigt, das Zertifikat zu nutzen.

Für Sperrungen nutzen Sie bitte die Web-Schnittstelle, unter der Sie auch den Zertifikatantrag gestellt haben, oder wenden Sie sich an den Teilnehmerservice Ihrer Einrichtung. Zusätzliche Kontaktinformationen sind unter https://www.pki.dfn.de/policies/informationen veröffentlicht.

Ein Zertifikat kann auch durch andere Personen außer Ihnen gesperrt werden, z. B. durch den Teilnehmerservice Ihrer Einrichtung oder die DFN-PCA.

Wurde Ihr Zertifikat gesperrt, so dürfen Sie dieses nicht weiter für Zwecke der Authentifizierung und Signatur verwenden. Die Verwendung zur Entschlüsselung von bereits verschlüsselten Daten ist hiervon nicht betroffen.

5 Angabe zum Grund einer Zertifikatsperrung

Wenn Sie Ihr Zertifikat sperren lassen, werden Sie nach einem Grund für die Sperrung gefragt. Sie müssen dabei Ihre Angabe nach dem folgenden Schema machen:

Schlüssel kompromittiert

Sie müssen den Sperrgrund "Schlüssel kompromittiert" bzw. "keyCompromise" wählen, wenn Sie Grund zu der Annahme haben, dass der private Schlüssel Ihres Zertifikats kompromittiert wurde, z. B. wenn eine unbefugte Person Zugriff auf den privaten Schlüssel hatte.

Änderung der Zugehörigkeit

Sie sollten den Sperrgrund "Änderung der Zugehörigkeit" bzw. "affiliationChanged" wählen, wenn sich der Name Ihrer Organisation oder andere organisatorische Informationen im Zertifikat geändert haben.

Ersetzt

Sie sollten den Sperrgrund "Ersetzt" bzw. "superseded" wählen, wenn sie ein neues Zertifikat beantragt haben, um Ihr bestehendes Zertifikat zu ersetzen.

Nicht mehr im Einsatz

Sie sollten den Sperrgrund "Nicht mehr im Einsatz" bzw. "cessationOfOperation" wählen, wenn Sie nicht mehr im Besitz aller Domainnamen des Zertifikats sind oder wenn Sie das Zertifikat nicht mehr verwenden, weil Sie die Website einstellen

Ohne Angabe

Wenn die vorigen Gründe nicht zutreffen, müssen Sie den Sperrgrund "Ohne Angabe" bzw. "unspecified" wählen.

6 Zertifikate für natürliche Personen (Nutzerzertifikate)

Wenn Sie ein Nutzerzertifikat einsetzen, müssen Sie die folgenden Bedingungen einhalten:

- Der private Schlüssel zu dem Zertifikat darf nur Ihnen zugänglich sein. Eine Weitergabe ist nicht erlaubt.
- Jedes Gerät, auf dem Sie den privaten Schlüssel speichern bzw. einsetzen, muss angemessen geschützt sein, also z. B. frei von Schadsoftware wie Viren sein und regelmäßig mit Sicherheits-Patches versehen werden.
- Sie dürfen den privaten Schlüssel nur dann an zentrale Geräte wie z.B. Mail-Appliances übergeben, wenn der Betreiber zusichert, die Regeln aus Kapitel 6, „Pflichten der Teilnehmer“ (https://www.pki.dfn.de/fileadmin/PKI/Pflichten-der-Teilnehmer.pdf), einzuhalten.
- Wenn Sie den privaten Schlüssel **nicht** auf einem Crypto-Token oder einer Smartcard speichern, also z. B. im Zertifikatsspeicher Ihres Betriebssystems, Ihres Browsers oder als Datei, so müssen Sie den privaten Schlüssel immer mit einer Passphrase schützen. Der private Schlüssel darf nicht unverschlüsselt und nicht ungeschützt vorliegen. Insbesondere muss bei Einsatz von Mozilla-Produkten ein „Master-Passwort“ gesetzt werden.
- Wenn Sie den privaten Schlüssel auf einem Crypto-Token bzw. einer Smartcard einsetzen, so muss das Token oder die Smartcard mit einer Passphrase/PIN geschützt sein.
- Die Passphrase/PIN darf nur Ihnen bekannt sein und muss mindestens 8 Zeichen lang sein.

7 Zertifikate für Datenverarbeitungssysteme (Server-Zertifikate)

Für Server-Zertifikate müssen folgende Bedingungen eingehalten werden:

- Das Zertifikat darf nur auf Datenverarbeitungssystemen installiert werden, die unter den im Zertifikat enthaltenen Namen erreichbar sind.
- Der private Schlüssel darf nur Administratoren der im Zertifikat genannten Server zugänglich sein.
- Jeder Server, auf dem der private Schlüssel vorgehalten wird, muss angemessen geschützt werden. Das heißt z. B.:
  - Der Server befindet sich in einer gesicherten Infrastruktur, z. B. hinter einer geeignet konfigurierten Firewall.
  - Der Server wird professionell betrieben, u. a. durch regelmäßiges Einspielen von Sicherheits-Patches.
  - Der administrative Zugriff auf den Server und somit auf den privaten Schlüssel ist klar geregelt.

Antragsteller bzw. Inhaber von Zertifikaten für Datenverarbeitungssysteme gestatten der DFN-Community-PKI, diese Zertifikate auf Systemen Dritter zum öffentlichen Abruf durch jedermann zu veröffentlichen, insbesondere im Rahmen von Certificate Transparency. Diese Veröffentlichung kann nicht rückgängig gemacht werden.

8 Zertifikate für Personengruppen (Gruppenzertifikate)

Wenn Sie ein Gruppenzertifikat einsetzen, muss dieses Dokument „Informationen für Zertifikatinhaber“ allen Gruppenmitgliedern bekannt gemacht werden.

Der private Schlüssel darf nur für Mitglieder der im Zertifikat benannten Personengruppe nutzbar sein.

Scheidet ein Mitglied aus der Personengruppe aus, so muss das Zertifikat gesperrt werden. Einzige mögliche Ausnahme: Hat das ausscheidende Mitglied den privaten Schlüssel ausschließlich auf einem Crypto-Token oder einer Smartcard mit nicht auslesbaren privaten Schlüsseln erhalten, die das Gruppenmitglied mit seinem Ausscheiden zurückgibt, so kann das Zertifikat weiter verwendet werden und braucht nicht gesperrt werden.

Darüber hinaus gelten die Regelungen für persönliche Zertifikate (siehe Abschnitt 5) entsprechend für alle Gruppenmitglieder.