Anleitung zur Nutzung der Webschnittstelle für Zertifikatanträge in der DFN-PKI

Inhalt

Inhalt

1 Registerkarte Zertifikate 4

1.1 Nutzerzertifikat 4
1.1.1 Zertifikatdaten - werden in das Zertifikat übernommen. 4
1.1.2 Weitere Angaben - werden nicht in das Zertifikat übernommen. 4
1.1.3 Schlüsselpaar generieren 5
1.1.4 Zertifikatantrag anzeigen, drucken und vom Teilnehmerservice prüfen lassen 6

1.2 Serverzertifikat 6
1.2.1 Zertifikatdaten - werden in das Zertifikat übernommen. 7
1.2.2 Weitere Angaben - werden nicht in das Zertifikat übernommen. 7
1.2.3 Schlüsselpaar generieren 8
1.2.4 Zertifikatantrag anzeigen, drucken und von der RA prüfen lassen 8

1.3 Zertifikat sperren 8

1.4 Zertifikat suchen 8

2 Registerkarte CA-Zertifikate 8

2.1 Wurzelzertifikat 8

2.2 DFN-PCA Zertifikat 8

2.3 CA-Zertifikat Ihrer Einrichtung 8

2.4 Zertifikatkette anzeigen 10

3 Registerkarte Gesperrte Zertifikate 10

3.1 Zertifikatsperrliste installieren 10

3.2 Zertifikatsperrliste anzeigen 10

4 Registerkarte Policies 10

4.1 DFN-PKI-Policy 10

5 Registerkarte Hilfe 10

6 Registerkarte Beenden 10

Webschnittstelle zur Beantragung von Zertifikaten

Jeder ausgelagerten Zertifizierungsstelle (CA) in der DFN-PKI steht eine Webschnittstelle zur Verfügung, über die bei dieser CA Zertifikate beantragt werden können. Über die Webschnittstelle können sowohl Nutzer- als auch Serverzertifikate beantragt werden.

Die URL der Webschnittstelle zur Beantragung von Zertifikaten hat immer die Form:

https://pki.pca.dfn.de/<CA der EINRICHTUNG>/pub

Dieses Dokument beschreibt die Funktionen der Webschnittstelle zur Beantragung von Zertifikaten für Nutzer und Administratoren in der Standardversion. In den Kap. 1.1 und 1.2 und wird die Beantragung eines Zertifikats ausführlich beschrieben. Erläuterungen zu den weiteren Funktionen dieser Schnittstelle finden Sie in den restlichen Kapiteln.

Bei Fragen rund um Zertifikate an Ihrer Einrichtung wenden Sie sich bitte an Ihren Teilnehmerservice.

1 Registerkarte Zertifikate

1.1 Nutzerzertifikat

Das folgende Beispiel zeigt, wie Sie ein **Nutzerzertifikat** beantragen können. Wählen Sie dafür bitte

- **Nutzerzertifikat**

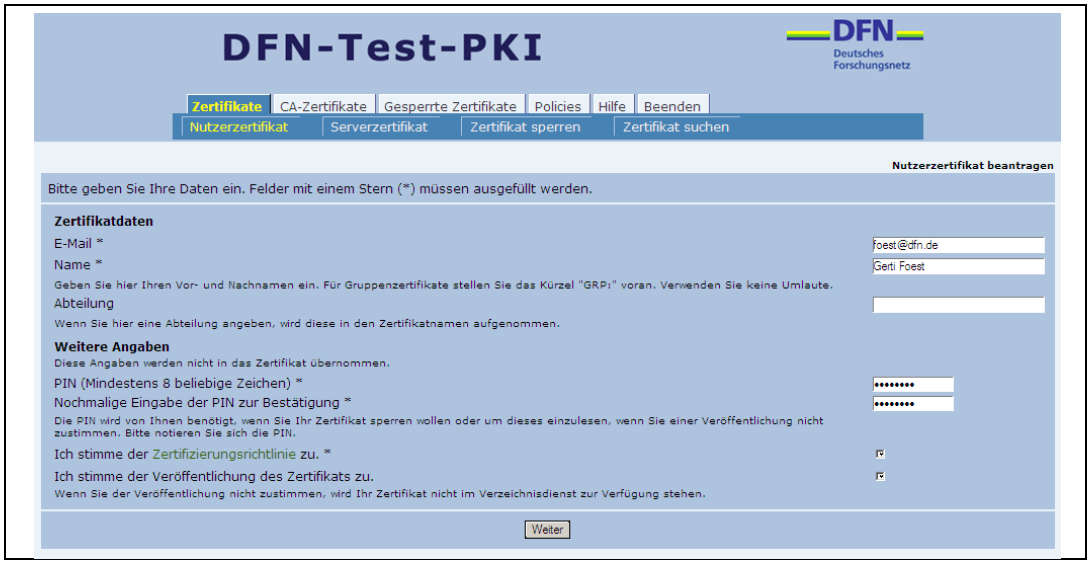

Abbildung 1: Formular zur Beantragung eines Nutzerzertifikats

Bitte füllen Sie in dem angezeigten Formular (Abbildung 1) alle mit einem * gekennzeichneten Felder aus**.**

1.1.1 Zertifikatdaten - werden in das Zertifikat übernommen**.**

- **E-Mail:** Tragen Sie hier bitte Ihre E-Mailadresse aus einer Domain Ihrer Einrichtung ein. E-Mailadressen aus anderen Domains (z.B. web.de, gmx.de, xyz.org) werden nur akzeptiert, wenn Ihre CA dem zugestimmt hat. Domains, für die keine Zustimmung vorliegt, werden abgewiesen.
- **Name:** Geben Sie bitte für Ihr persönliches Zertifikat Ihren Vor- und Nachnamen an. Namenszusätze, die im amtlichen Ausweispapier geführt werden (z.B. "Dr."), können ebenfalls angegeben werden. in den CN aufgenommen werden. Namenszusätze, die nicht im amtlichen Ausweispapier geführt werden (z.B. "Prof.") dürfen nicht verwendet werden.
  Gruppenzertifikaten und Pseudonymzertifikaten stellen Sie bitte das Kürzel „GRP:" bzw. „PN:" voran.
- **Abteilung:** Im diesem Feld sollten Sie nur dann Angaben machen, wenn die Abteilung im "OU=" – Feld des Zertifikats erscheinen soll. Es dürfen keine Umlaute verwendet werden.

1.1.2 Weitere Angaben - werden nicht in das Zertifikat übernommen.

- Die **PIN** benötigen Sie als Passwort beim Importieren Ihres Zertifikats, wenn Sie einer Veröffentlichung nicht zugestimmt haben oder wenn Sie Ihr Zertifikat sperren wollen. Sie sollten sich deshalb die PIN unbedingt notieren.
- **Einhaltung der Zertifizierungsrichtlinie.** Sie müssen der Zertifizierungsrichtlinie zustimmen, da Ihr Antrag sonst nicht bearbeitet werden kann.

- **Veröffentlichung des Zertifikats.** Wenn Sie der Veröffentlichung zustimmen, wird Ihr Zertifikat im Verzeichnisdienst (LDAP) der DFN-PKI eingetragen, der im Internet frei zugänglich ist. Wenn Sie der Veröffentlichung nicht zustimmen, benötigen Sie zum Import Ihres Zertifikats die oben eingetragene PIN.
    - Sie können Ihre Zustimmung zur Veröffentlichung Ihres Zertifikats jederzeit mit Wirkung für die Zukunft durch eine E-Mail an dfnpca@dfn-cert.de widerrufen.
    - Wenn Sie der Veröffentlichung Ihres Zertifikats nicht zustimmen, kann dies nachträglich nicht geändert werden. Sie müssen dann ein neues Zertifikat beantragen und dafür der Veröffentlichung zustimmen.

Wenn Sie *Weiter* betätigen, werden Ihnen Ihre Angaben noch einmal angezeigt. Sie können die Angaben dann ändern oder die Richtigkeit bestätigen.

1.1.3 Schlüsselpaar generieren

Wenn Sie Ihre Angaben *Bestätigen*, wird Ihr Schlüsselpaar (Schlüssellänge 2048 Bit) für das beantragte Zertifikat im Browser generiert. Der Vorgang wird in den Browsern unterschiedlich angezeigt.

Abbildung 2: Anzeige der Eingabedaten u. Schlüsselerzeugung Mozilla Firefox

In **Mozilla Firefox** wird nur kurz ein kleines Fenster eingeblendet (Abbildung 2).

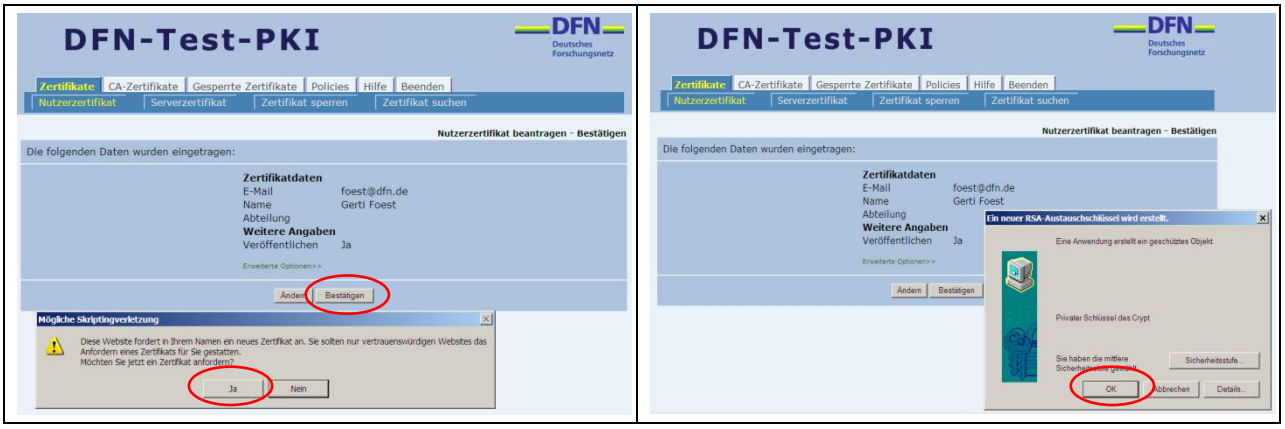

Abbildung 3: Anzeige der Eingabedaten u. Schlüsselerzeugung Internet Explorer

Im **Internet Explorer (IE)** werden Sie in zwei Schritten aufgefordert, der Zertifikatanforderung zuzustimmen (Abbildung 3).

Bitte antworten Sie jeweils mit "Ja" bzw. "Ok".

Der IE erzeugt Ihr Schlüsselpaar standardmäßig (wie Mozilla) im Browser, das Schlüsselpaar kann aber unter "Erweiterte Optionen" auch auf einem kryptographischen Gerät (z.B. SmartCard) erzeugt werden.

1.1.4 Zertifikatantrag anzeigen, drucken und vom Teilnehmerservice prüfen lassen

Nach der Schlüsselerzeugung werden Sie aufgefordert, sich Ihren Zertifikatantrag anzeigen zu lassen (PDF-Datei) und ihn auszudrucken (Abbildung 4).

Bitte vervollständigen Sie nun die Angaben auf dem ausgedruckten Zertifikat und unterschreiben Sie ihn. Dann legen Sie den Zertifikatantrag zusammen mit Ihrem Personalausweis oder Reisepass beim Teilnehmerservice Ihrer Einrichtung zur Prüfung und weiteren Bearbeitung vor.

Abbildung 4: Zertifikatantrag anzeigen

1.2 Serverzertifikat

Das folgende Beispiel zeigt, wie Sie ein **Serverzertifikat** beantragen können. Wählen Sie dafür bitte

- **Serverzertifikat**

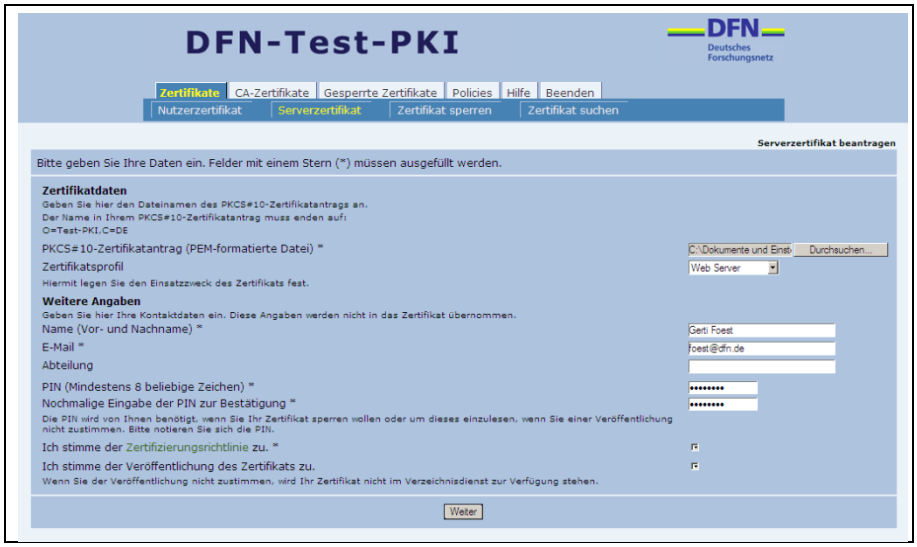

Abbildung 5: Formular zur Beantragung eines Serverzertifikats

Bitte füllen Sie in dem angezeigten Formular (Abbildung 5) alle mit einem * gekennzeichneten Felder aus.

1.2.1 Zertifikatdaten - werden in das Zertifikat übernommen.

- **Dateiname**. Die Zertifikatdaten für Serverzertifikate werden nicht über die Webschnittstelle eingegeben, sondern sind als sogenannter PKCS#10-Antrag in einer Datei enthalten, die vorher erzeugt werden muss. Wie bei Ihrer Server-Software ein PKCS#10-Antrag erzeugt werden kann, entnehmen Sie bitte der entsprechenden Dokumentation Ihrer Software.

  Ein PKCS#10-Antrag kann auch mit der Software 'openssl' mit folgendem Kommando erzeugt werden. Auf den Webseiten der DFN-PKI finden Sie eine Anleitung zur Nutzung von OpenSSL:

  https://www.pki.dfn.de/fileadmin/PKI/anleitungen/Anleitung_Nutzung_OpenSSL.pdf

- **Zertifikatprofil.** Hier können Sie angeben, für welche Anwendung Sie das Zertifikat beantragen, damit die entsprechenden Extensions in das Zertfikat eingetragen werden. Standardmäßig wird hier der Typ *Web Server* ausgewählt.

  Eine Beschreibung der Zertifikatprofile mit den entsprechenden Anwendungsbereichen finden Sie auf den Webseiten der DFN-PKI:

  https://www.pki.dfn.de/fileadmin/PKI/anleitungen/DFN-PKI-Zertifikatprofile_Global.pdf

1.2.2 Weitere Angaben - werden nicht in das Zertifikat übernommen.

- **Name und E-Mailadresse.** Bei der Beantragung eines Serverzertifikats müssen Sie hier Ihren Vor- und Nachnamen und Ihre E-Mailadresse angeben, damit die Zertifizierungsstelle das Serverzertifikat einem Ansprechpartner zuordnen kann.
- Die **PIN** benötigen Sie zum Import Ihres Zertifikats und wenn Sie das Zertifikat sperren wollen.
- **Einhaltung der Zertifizierungsrichtlinie.** Sie müssen der Zertifizierungsrichtlinie zustimmen, da Ihr Antrag sonst nicht bearbeitet werden kann.

Abbildung 6: Anzeige der Angaben für ein Serverzertifikat

Wenn Sie *Weiter* betätigen, werden Ihnen Ihre Angaben noch einmal angezeigt. Sie können die Angaben dann ändern oder die Richtigkeit bestätigen.

1.2.3 Schlüsselpaar generieren

Wenn Sie Ihre Angaben *Bestätigen*, wird Ihr Schlüsselpaar (Schlüssellänge 2048 Bit) für das beantragte Zertifikat im Browser generiert. Der Vorgang wird in den Browsern unterschiedlich angezeigt (s. Kap. 1.1.3.).

1.2.4 Zertifikatantrag anzeigen, drucken und vom Teilnehmerservice prüfen lassen

Nach der Schlüsselerzeugung werden Sie aufgefordert, sich Ihren Zertifikatantrag anzeigen zu lassen (PDF-Datei) und ihn auszudrucken (Abbildung 4).

Bitte vervollständigen Sie nun die Angaben auf dem ausgedruckten Zertifikat und unterschreiben Sie ihn. Dann legen Sie den Zertifikatantrag zusammen mit Ihrem Personalausweis oder Reisepass bei dem Teilnehmerservice Ihrer Einrichtung zur Prüfung und weiteren Bearbeitung vor.

1.3 Zertifikat sperren

Hier können Sie bereits ausgestellte Zertifikate wieder sperren lassen. Dazu benötigen Sie die Seriennummer des Zertifikats, die Sie mit Ihrem Zertifikat erhalten haben. Außerdem benötigen Sie die **PIN**, die Sie in Ihrem Zertifikatantrag angegeben haben.

1.4 Zertifikat suchen

Hier können Sie nach Zertifikaten suchen, die von der CA Ihrer Einrichtung ausgestellt wurden und die Sie z.B. für Ihre E-Mail-Kommunikation herunterladen möchten. Sie können als Suchkriterium den Namen oder die E-Mail eingeben.

2 Registerkarte CA-Zertifikate

2.1 Wurzelzertifikat

Hier können Sie das Wurzelzertifikat der DFN-PKI herunterladen. Dieses Zertifikat ist in allen gängigen Browsern sowie in einer Reihe weiterer Anwendungen bereits fest integriert. Mehr zur Integration des DFN-PKi Wurzelzertifikats finden Sie auf den Webseiten der DFN-PKI unter

https://www.pki.dfn.de/die-cas-im-dfn/integration-dfn-pki/

2.2 DFN-PCA Zertifikat

Hier können Sie das Zertifikat der DFN-Verein PCA Global - 01, herunterladen. Diese CA stellt alle weiteren CA-Zertifikate in der DFN-PKI aus.

2.3 CA-Zertifikat Ihrer Einrichtung

Hier können Sie das CA-Zertifikat Ihrer Einrichtung herunterladen. Diese CA stellt die Nutzer- und Serverzertifikate für Ihre Einrichtung aus.

Die **Vorgehensweise des Herunterladens** ist in allen Fällen gleich. Abhängig von den verwendeten Browsern werden Sie zu weiteren Aktionen aufgefordert.

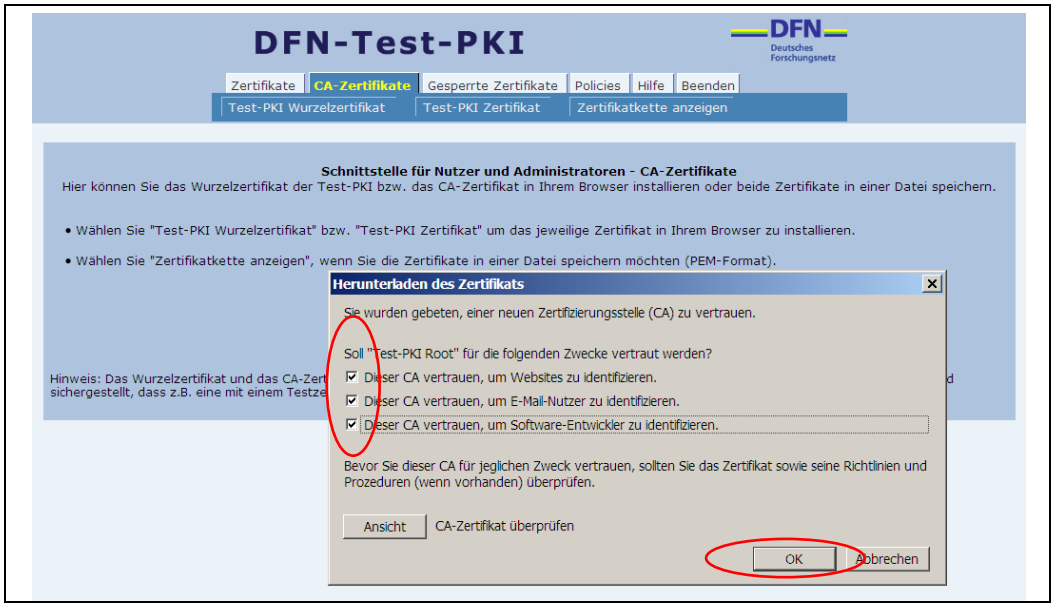

Abbildung 7: Laden des Root- bzw. CA-Zertifikats Mozilla Firefox

Wenn Sie in **Mozilla Firefox** (Abbildung 7) eine der Registerkarten anklicken, wird das entsprechende CA-Zertifikat direkt in Ihren Browser geladen. Sie können dann wählen, für welche Zwecke Sie der jeweiligen Zertifizierungsstelle vertrauen wollen. In der Regel sollten Sie alle Kästchen ankreuzen. Wenn Sie die Zertifikate auch in andere Anwendungen (E-Mail etc.) importieren möchten, gehen Sie mit der rechten Maustaste auf die entsprechende Registerkarte und wählen "Ziel Speichern unter". Das Zertifikat wird dann im Zielordner abgelegt und kann in andere Programme importiert werden.

Sie erhalten von Mozilla Firefox keine Meldung über die erfolgreiche Installation im Browser. Überprüfen Sie deshalb die Installation der Zertifikate über:

Extras -> Einstellungen -> Erweitert -> Zertifikate anzeigen -> Zertifizierungsstellen. Dort müssen jetzt das importierte CA-Zertifikat eingetragen sein.

Der **Internet Explorer** fordert Sie in mehreren Schritten auf, das Zertifikat zu importieren (Abbildung 8). Öffnen Sie das Zertifikat, wenn Sie es nur in Ihrem Browser installieren wollen. Sie können das Zertifikat auch speichern und dann in Ihren Browser und in andere Programme importieren. Wenn Sie das Zertifikat installieren, werden Sie durch einen Assistenten geführt und die erfolgreiche Installation wird Ihnen angezeigt.

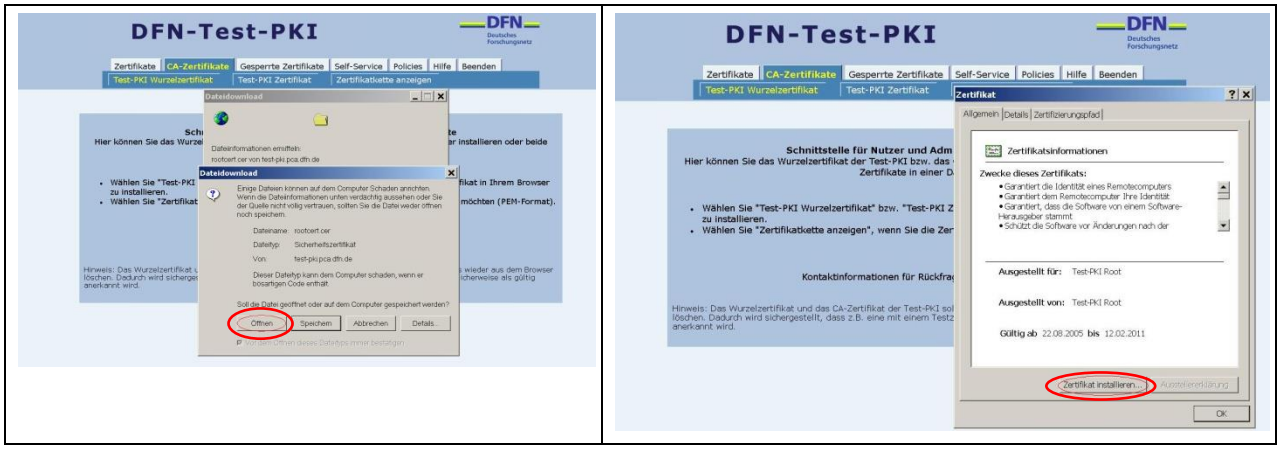

Abbildung 8: Laden des Root- bzw. CA-Zertifikats Internet Explorer

2.4 Zertifikatkette anzeigen

Hier können Sie sich die gesamte Zertifikatkette - das Telekom Root CA2 Zertifikat, das Zertifikat der DFN-Verein PCA Global – 01 und das CA-Zertifikat Ihrer Einrichtung – anzeigen lassen (PEM-Format) und in einer Datei speichern.

3 Registerkarte Gesperrte Zertifikate

3.1 Zertifikatsperrliste installieren

Hier können Sie sich die aktuelle Zertifikatsperrliste in Ihren Browser laden. Der Internet Explorer bietet Ihnen zusätzlich die Möglichkeit, die Zertifikatsperrliste zu speichern, um sie auch in andere Anwendungen zu importieren.

3.2 Zertifikatsperrliste anzeigen

Hier können Sie sich die aktuelle Zertifikatsperrliste anzeigen lassen und in einer Datei speichern.

4 Registerkarte Policies

4.1 DFN-PKI-Policy

Hier können Sie sich die Policy (Zertifizierungsrichtlinie) der DFN-PKI ansehen und herunterladen.

5 Registerkarte Hilfe

Hier finden Sie in der Regel eine Nutzeranleitung und die Ansprechpartner Ihrer Einrichtung für alle Fragen rund um Zertifikate.

6 Registerkarte Beenden

Hier können Sie die Webschnittstelle für Nutzer und Administratoren verlassen.