

Nutzerzertifikat beantragen

Die Beantragung eines Nutzerzertifikates erfolgt im Web-Browser (z.B. Firefox) über die Webseite der DFN-PKI.

Während der Beantragung des Zertifikates werden ein geheimer Schlüssel und ein öffentlicher Schlüssel in ihrem Webbrowser erzeugt. Aus dem öffentlichen Schlüssel wird zusammen mit Metadaten (z.B. Ihr Name und Ihre E-Mail Adresse) ein Zertifikat erzeugt. Nach erfolgreicher Ausstellung des Zertifikates, können Sie das Zertifikat ebenfalls in den Webbrowser importieren und mit dem geheimen Schlüssel *kombinieren*.

Das Nutzerzertifikat kann zum digitalen Signieren und Verschlüsseln von E-Mails genutzt werden. Da in unserem E-Mail-System die E-Mail-Adressen zur Zeit nicht in der Form Vorname.Nachname@FB.hs-fulda.de vorliegen, kann das Zertifikat für diese Zwecke nicht mit dem GroupWise-Client genutzt werden, möglich ist die Nutzung jedoch mit anderen E-Mail-Clients, wie Thunderbird oder Outlook.

Die Ausstellung von Nutzerzertifikaten erfordert die persönliche Prüfung der Identität durch Vorlage eines Ausweisdokuments im Rechenzentrum.

Durch die Beantragung eines Nutzer-Zertifikates sind Sie verpflichtet, die Regelungen und Pflichten von Zertifikatsinhabern in der DFN-PKI zu befolgen. Diese finden Sie unter

<https://www.pki.dfn.de/fileadmin/PKI/Info-fuer-Zertifikatinhaber.pdf>.

Master-Passwort für Firefox setzen

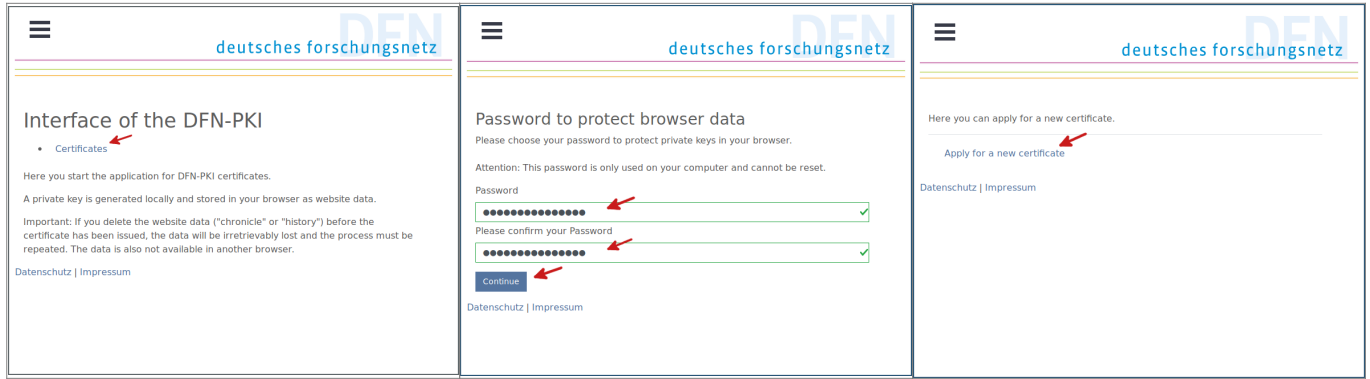
Firefox und Thunderbird schützen sensible Daten nur dann richtig, wenn Sie ein Master-Passwort benutzen. Sie sollten daher bei Mozilla-Produkten (Firefox und/oder Thunderbird) zuerst ein Master-Passwort setzen, bevor Sie einen privaten Schlüssel erzeugen oder importieren. Klicken Sie in der rechten oberen Ecke von Firefox auf das Icon mit den drei waagerechten Linien und dann auf *Einstellungen*.

Wählen Sie den Bereich *Sicherheit* aus und setzen Sie dann im Bereich *Passwörter* einen Haken vor *Master-Passwort verwenden*. Danach öffnet sich ein Fenster, in dem Sie das Master-Passwort initial festlegen können.

Zertifikat beantragen

Ein CA-Zertifikat kann über die CA-Web-Seite der Hochschule Fulda beantragt werden. Rufen Sie dafür die Webseite <https://pki.pca.dfn.de/dfn-pki/dfn-ca-global-g2/2570> auf und folgen Sie den Anweisungen auf der Webseite.

Um das Zertifikat in ihrem Browser, sowie den gesamten Bestellprozess zu sichern, legen Sie zu Beginn (mittleres Bild) ein Passwort fest. Dieses Passwort benötigen Sie später erneut, um ihr Zertifikat nach der Ausstellung zu speichern.



Füllen Sie nun das Formular für die Metadaten ihres Zertifikates aus. Hier werden zunächst ihr **Name**, ihre **E-Mail Adresse** und (optional) ihre Abteilung abgefragt. Bei *Namespace* wählen Sie bitte **O=Hochschule Fulda,L=Fulda,ST=Hessen,C=DE**.

Legen Sie außerdem ein Passwort fest, mit dem Sie ihr Zertifikat im Falle des Verlustes oder Diebstals zurückziehen können. Setzen Sie abschließend die beiden Häkchen und klicken Sie auf *Submit*.

New certificate

Here you can apply for a new certificate.

Zertifikatdaten

Here you can apply for a new certificate.

Certificate profile **User** ?

Neuer Antrag

Create certificate request

The following data is used to generate a new certificate request.

► E-mail addresses with the following domain names can be used without further confirmation. E-mail addresses with other domain names must be confirmed separately:

Name
Sven Reissmann ✓

E-Mail
sven.reissmann@rz.hs-fulda.de ✓

Department (optional)
RZ ✓

Namespace
O=Hochschule Fulda,L=Fulda,ST=Hessen,C=DE

Ihre Daten

Enter further data below. What you enter here will not be found in the certificate.

Revoke-PIN
●●●●●●●●●● ✓

Revoke-PIN - Confirmation
●●●●●●●●●● ✓

This PIN is required if you want to revoke your certificate. Please make a note of this PIN.

I am committed to comply with the regulations contained in [Informationen für Zertifikatinhaber](#).

Optional: I agree to the [publication of the certificate](#) with the contained names and e-mail addresses. You can withdraw this agreement by sending an e-mail to pki@dfn.de.

Nach dem Absenden des Formulars sehen Sie eine Übersicht ihrer Angaben und haben die Möglichkeit, einen Zertifikatantrag anzuzeigen. Bitte drucken Sie diesen Antrag aus und bringen Sie diesen unterschrieben und zusammen mit einem Ausweisdokument zur Verifikation im Rechenzentrum vorbei.

New certificate

Here you can apply for a new certificate.

Zertifikatdaten

Here you can apply for a new certificate.

Certificate profile **User** ?

Neuer Antrag

Create certificate request

The following data is used to generate a new certificate request.

► E-mail addresses with the following domain names can be used without further confirmation. E-mail addresses with other domain names must be confirmed separately:

Name
Sven Reissmann ✓

E-Mail
sven.reissmann@rz.hs-fulda.de ✓

Department (optional)
RZ ✓

Namespace
O=Hochschule Fulda,L=Fulda,ST=Hessen,C=DE

Ihre Daten

Enter further data below. What you enter here will not be found in the certificate.

Revoke-PIN
●●●●●●●● ✓

Revoke-PIN - Confirmation
●●●●●●●● ✓

This PIN is required if you want to revoke your certificate. Please make a note of this PIN.

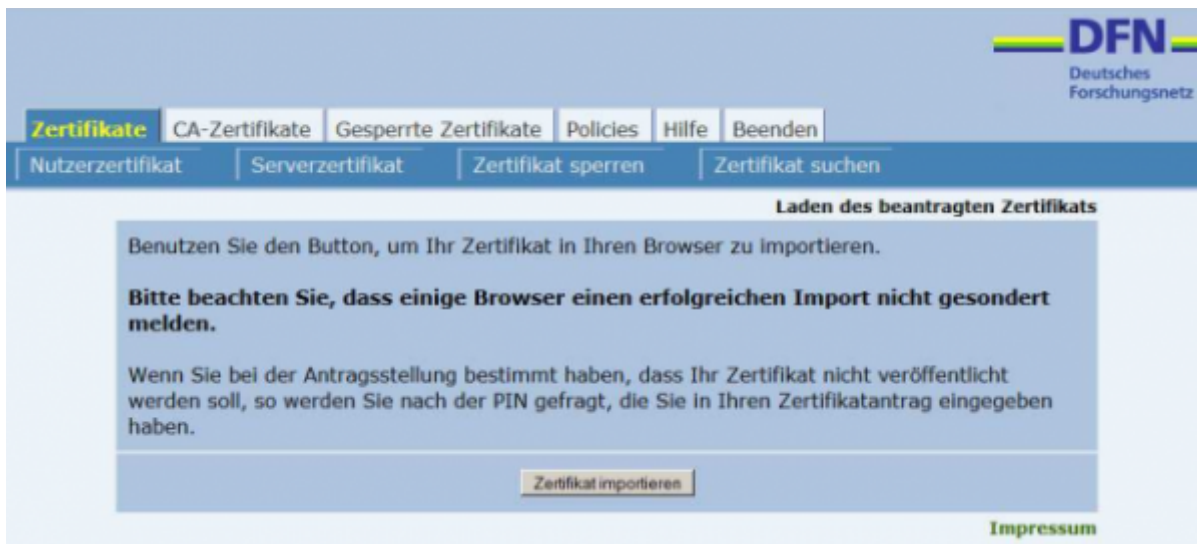
I am committed to comply with the regulations contained in [Informationen für Zertifikatinhaber](#).

Optional: I agree to the publication of the certificate with the contained names and e-mail addresses. You can withdraw this agreement by sending an e-mail to pki@dfn.de.

Der private Schlüssel für das Zertifikat wurde im Browser erzeugt und gespeichert, so dass der zertifizierte öffentliche Schlüssel später nur in dem Browser importiert werden kann, von dem das Zertifikat beantragt worden ist.

Zertifikat importieren

Nachdem Ihr Zertifikatantrag bearbeitet wurde, erhalten Sie eine E-Mail, in der ihr Zertifikat enthalten ist. Klicken Sie auf die Web-Adresse für Ihr Zertifikat, die Ihnen mit der Bestätigungs-Mail zugeschickt worden ist und dann auf *Zertifikat importieren*.



Sie werden jetzt aufgefordert, das Master-Passwort einzugeben, das Sie zuvor festgelegt haben. Danach wird das Zertifikat in Ihren Browser importiert und kann ab sofort benutzt werden.

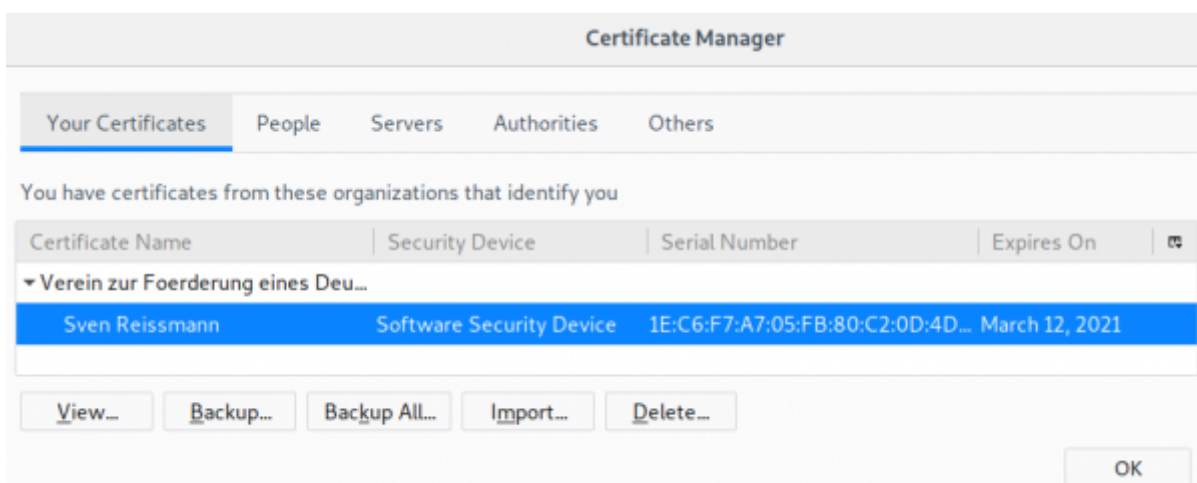
Falls Sie versuchen, das Zertifikat in einem Browser zu importieren, von dem Sie das Zertifikat nicht beantragt haben, erhalten Sie eine Fehlermeldung, da in diesem Browser kein passender privater Schlüssel hinterlegt ist.

Backup des Zertifikats erstellen

Ihr Zertifikat befindet sich nun ausschließlich in dem Webbrowser, mit dem Sie es beantragt haben. Sie sollten daher unbedingt ein Backup erstellen. Dieses backup können Sie anschließend auch verwenden, um das Zertifikat auch in andere Browser oder ih Ihren E-Mail Client zu importieren.

Klicken Sie wieder in der rechten oberen Ecke von Firefox auf das Icon mit den drei waagerechten Linien und dann auf *Einstellungen*. Wählen Sie den Bereich *Erweitert* und dann den Reiter *Zertifikate* aus. Klicken Sie anschließend auf *Zertifikate anzeigen*. Danach wird Ihnen das Fenster des Zertifikat-Managers angezeigt.

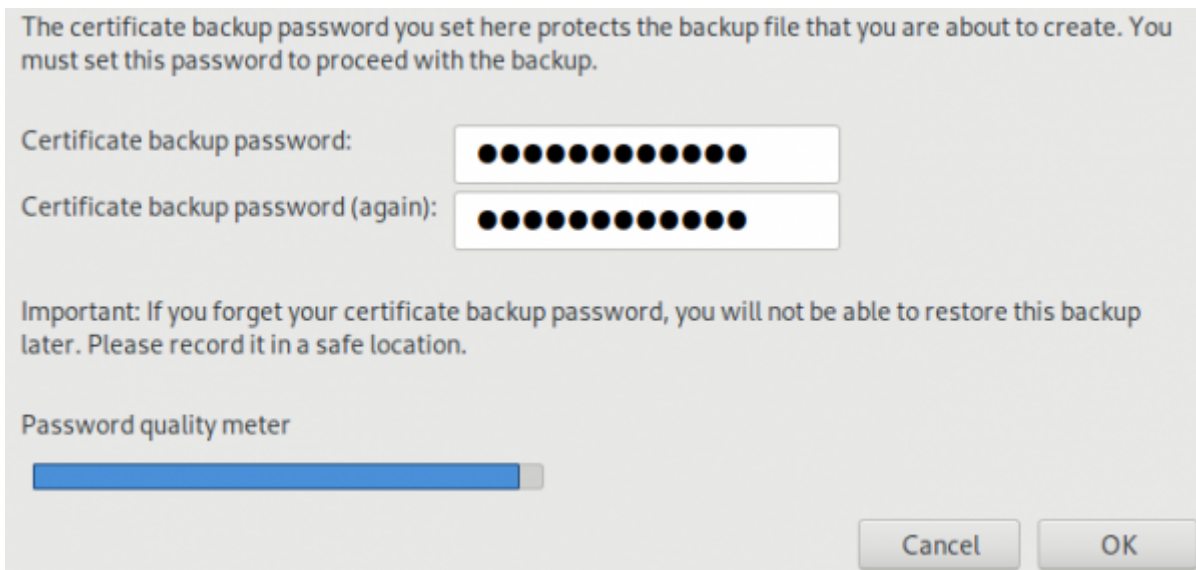
Wählen Sie ihr Zertifikat aus und klicken Sie dann auf *Sichern....* Wählen Sie ein Verzeichnis und einen Namen für die Datei und klicken Sie dann auf *Speichern*.



Sie werden unter Umständen zuerst nach dem Master-Passwort für Firefox gefragt, das Sie weiter

oben festgelegt haben.

Anschließend müssen Sie ein Passwort für die Backup-Datei festlegen, in der Sie das Zertifikat speichern wollen. Denken Sie daran, dass Sie ein gutes Passwort wählen, das den Richtlinien der Hochschule Fulda entspricht.



Bewahren Sie die Backup-Datei auf.

Zertifikat in E-Mail Client importieren

Wenn Sie Ihr Zertifikat für die Verschlüsselung und Signatur von E-Mails nutzen möchten, müssen Sie dieses in Ihr E-Mail Programm (z.B. Thunderbird) importieren. Sie können dafür die Backup-Datei aus dem vorigen Schritt verwenden. Die Nutzung des Zertifikats im GroupWise-Client ist vorerst nicht möglich, da die E-Mail-Adressen in GroupWise nicht der E-Mail-Adresse im Zertifikat (Vorname.Nachname@FB.hs-fulda.de) entsprechen.

Dieser Teil unserer Dokumentation ist noch unvollständig. Eine detaillierte Anleitung finden Sie in diesem Dokument:

s_mime_beantragung_und_nutzung.pdf

From: <https://doku.rz.hs-fulda.de/> - **Dokumentation des Rechenzentrums**

Permanent link: <https://doku.rz.hs-fulda.de/doku.php/docs:dfnpki:clientzertifikat>

Last update: **20.12.2019 16:33**

