SHORTGUIDE
BEANTRAGUNG EINES PERSÖNLICHEN NUTZER-ZERTIFIKATS

FÜR MITGLIEDER UND ANGEHÖRIGE DER RUB

Persönliche Nutzerzertifikate

Das digitale Zertifikat ist ein Datensatz, der die Identität des Inhabers bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Zertifikate sind Grundlagen für digitale Signaturen und Verschlüsselung und bilden somit die Grundlage sicherer Kommunikation im Netz.

Die Nutzerzertifikate stehen allen Mitgliedern und Angehörigen der RUB zur Verfügung. Persönliche Nutzerzertifikate eignen sich für das Signieren (z.B. von E-Mails) sowie zur Verschlüsselung und Authentifizierung.

Wie entsteht mein Nutzerzertifikat?

Sie beantragen Ihr Nutzerzertifikat in Ihrem Browser. Der Browser erzeugt dabei ein Schlüsselpaar: Der geheime (private) Teil des Schlüssels verbleibt im Browser, der öffentliche Teil des Schlüssels wird dem DFN-Verein übermittelt. IT.SERVICES gibt Ihren Antrag nach Identitätsprüfung frei. Der DFN-Verein benachrichtigt Sie per E-Mail, sobald das Zertifikat beglaubigt ist. Erst durch die Zusammenführung des geheimen Schlüssels und des durch den DFN beglaubigten Teils in Ihrem Browser entsteht das Zertifikat. Dieses kann exportiert werden, um sicher abgelegt und in anderen Programmen verwendet werden zu können.

Die nachfolgende Anleitung beschreibt Ihnen Schritt für Schritt, wie Ihr persönliches Nutzerzertifikat beantragt, ausgestellt und gesichert wird.

Beantragung eines persönlichen Nutzerzertifikats

Die Beantragung erfolgt über das DFN-PKI-Portal:

https://pki.pca.dfn.de/uni-bochum-ca-g2/pub

Bei Fragen können Sie Kontakt mit der Registrierungsstelle aufnehmen: pki@ruhr-uni-bochum.de oder telefonisch im Servicecenter unter 0234/32-24025.

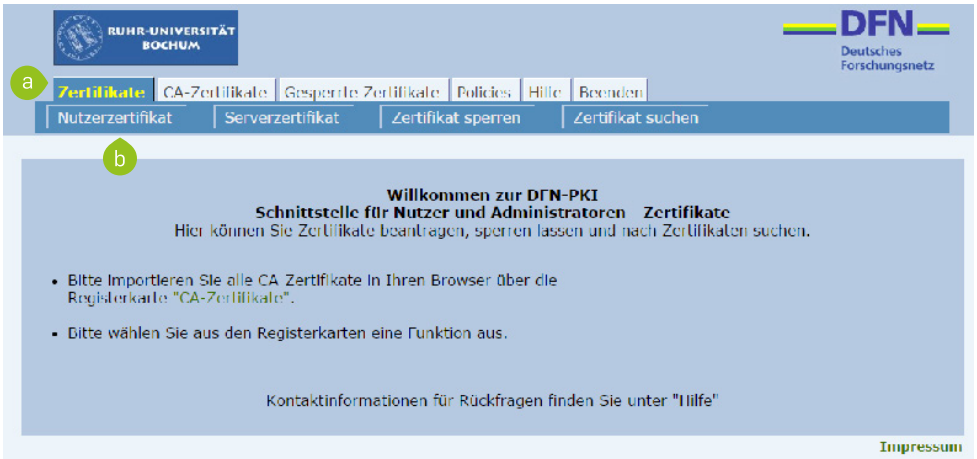
Hinweis:

Für Gruppenzertifikate stellen Sie das Kürzel „GRP:“ voran

BEANTRAGUNG, AUSSTELLUNG & SICHERUNG

Schritt 1

Bentragen Sie Ihr persönliches Zertifikat, indem Sie das DFN-PKI-Portal aufrufen und zu Zertifikate (a) und Nutzerzertifikat (b) gehen.



Hinweis

Beantragen Sie das Zertifikat auf einem vertrauenswürdigen PC, auf den nur Sie Zugriff haben, da im Browser Teil 1 des Zertifikats (privater Schlüssel) erzeugt und gespeichert wird.

Schritt 2

Füllen Sie den Antrag aus und klicken auf „Weiter“. Überprüfen Sie Ihre Angaben. Nach der Bestätigung erzeugt Ihr Browser das Schlüsselpaar und übermittelt dem DFN-Verein Ihren öffentlichen Schlüssel (Teil 2) zur Signierung.

Ihr Browser zeigt Ihnen jetzt den zugehörigen Zertifikatsantrag an, den Sie bitte ausdrucken und unterschreiben.

Schritt 3

Kommen Sie mit dem unterzeichneten Zertifikatsantrag in das Servicecenter der IT.SERVICES und reichen den Antrag persönlich unter Vorlage eines amtlichen Lichtbildausweises (Personalausweis oder Reisepass) ein.

Die Registrierungsstelle finden Sie bei den

IT.SERVICES
Servicecenter
Gebäude NA 02/297
Mo–Fr 10.00–15.30 Uhr

Bei Fragen können Sie Kontakt mit der Registrierungsstelle aufnehmen: pki@ruhr-uni-bochum.de oder telefonisch unter 0234/32-24025.

Schritt 4

Das signierte Zertifikat bekommen Sie per E-Mail zugestellt. Öffnen Sie den enthaltenen Link in dem Browser, in dem Sie den Zertifikatsantrag erstellt haben, da sich hier bereits Teil 1 (privater Schlüssel) des Zertifikats befindet. **Importieren** Sie dieses Zertifikat in den Browser.

Schritt 5

Das **Sichern Ihres persönlichen Nutzerzertifikats** ist wichtig, denn es befindet sich in dem Web-Browser, den Sie beim Erzeugen des Zertifikats verwendet haben. Das Exportieren und Sichern ist zudem wichtig, um das Zertifikat in anderen Programmen und auf mobilen Geräten nutzen zu können.

Internet Explorer: Interneteinstellungen ▸ Inhalte ▸ Zertifikate ▸ „Zertifikate“ anklicken.

- Unter „Eigene Zertifikate“ wählen Sie Ihr Nutzerzertifikat aus und klicken auf „Exportieren“. Der Zertifikatexport-Assistent stellt Ihnen die Frage, ob Sie auch den privaten Schlüssel exportieren möchten. Wählen Sie „Ja, privaten Schlüssel exportieren“.
- Wählen Sie im nächsten Schritt das Format „Privater Informationsaustausch - PKCS #12 (.PFX)“ aus und aktivieren Sie das Häkchen „Alle erweiterten Eigenschaften exportieren“.
- Geben Sie im folgenden Schritt ein sicheres Kennwort für die Sicherung Ihres Benutzerzertifikats ein. Mit diesem Kennwort ist die Sicherungsdatei geschützt. Sie werden es eingeben müssen, wenn Sie die Sicherungsdatei später an einer anderen Stelle importieren (zum Beispiel in Ihrem Mail-Klienten).
- Geben Sie anschließend einen Dateinamen an. Wählen Sie einen sicheren Speicherort für die Datei aus, zum Beispiel einen USB-Stick, den Sie sicher verwahren. Wählen Sie auf keinen Fall einen für andere zugänglichen Speicherort aus!
- Schließen Sie den Assistenten ab, um die Datei zu sichern.

Mozilla Firefox: Einstellungen ▸ Sicherheit

- Setzen Sie ein Häkchen bei „Master-Passwort“ und vergeben Sie ein Passwort (falls noch nicht geschehen).
- Klicken Sie auf den Bereich „Erweitert“, wählen Sie „Zertifikate“ und klicken auf „Zertifikate anzeigen“.
- Unter „Ihre Zertifikate“ sehen Sie Ihr Benutzerzertifikat. Wählen Sie es aus und klicken Sie auf „Sichern“.
- Geben Sie einen Dateinamen an. Wählen Sie einen sicheren Speicherort für die Datei aus, zum Beispiel einen USB-Stick, den Sie sicher verwahren. Wählen Sie auf keinen Fall einen für andere zugänglichen Speicherort aus!
- Klicken Sie auf „Speichern“ und geben Sie zunächst das Master-Passwort ein, um den Schlüsselbund zu entsperren. Geben Sie danach ein sicheres Kennwort für die Sicherung Ihres Benutzerzertifikats ein. Mit diesem Kennwort ist die Sicherungsdatei geschützt. Sie werden es eingeben müssen, wenn Sie die Sicherungsdatei später an einer anderen Stelle importieren (zum Beispiel in Ihrem Mail-Klienten).

Safari/ Apple Mac OS: Schlüsselbundverwaltung ▸ Schlüssel

- Suchen Sie Ihr Nutzerzertifikat in der Liste. Es hat Ihren Namen.
- Klicken Sie mit rechts auf das Zertifikat und wählen Sie „Exportieren“.
- Unter „Ihre Zertifikate“ sehen Sie Ihr Benutzerzertifikat. Wählen Sie es aus und klicken Sie auf „Sichern“.
- Geben Sie einen Dateinamen an. Wählen Sie einen sicheren Speicherort für die Datei aus, zum Beispiel einen USB-Stick, den Sie sicher verwahren. Wählen Sie auf keinen Fall einen für andere zugänglichen Speicherort aus!
- Klicken Sie auf „Sichern“ und geben Sie im folgenden Schritt ein sicheres Kennwort für die Sicherung Ihres Benutzerzertifikats ein. Mit diesem Kennwort ist die Sicherungsdatei geschützt. Sie werden es eingeben müssen, wenn Sie die Sicherungsdatei später an einer anderen Stelle importieren (zum Beispiel in Ihrem Mail-Klienten)

Google Chrome: Einstellungen ▸ HTTPS/SSL ▸Zertifikate verwalten ▸ Exportieren

- Unter „Eigene Zertifikate“ wählen Sie Ihr Nutzerzertifikat aus und klicken auf „Exportieren“. Der Zertifikatexport-Assistent stellt Ihnen die Frage, ob Sie auch den privaten Schlüssel exportieren möchten. Wählen Sie „Ja, privaten Schlüssel exportieren“.
- Wählen Sie im nächsten Schritt das Format „Privater Informationsaustausch - PKCS #12 (.PFX)“ aus und aktivieren Sie das Häkchen „Alle erweiterten Eigenschaften exportieren“.
- Geben Sie im folgenden Schritt ein sicheres Kennwort für die Sicherung Ihres Benutzerzertifikats ein. Mit diesem Kennwort ist die Sicherungsdatei geschützt. Sie werden es eingeben müssen, wenn Sie die Sicherungsdatei später an einer anderen Stelle importieren (zum Beispiel in Ihrem Mail-Klienten).
- Geben Sie anschließend einen Dateinamen an. Wählen Sie einen sicheren Speicherort für die Datei aus, zum Beispiel einen USB-Stick, den Sie sicher verwahren. Wählen Sie auf keinen Fall einen für andere zugänglichen Speicherort aus!
- Schließen Sie den Assistenten ab, um die Datei zu sichern.

Hinweis

Wenn es Probleme mit der Authentifizierung oder Überprüfung der Signatur gibt, prüfen Sie, ob alle Zertifikate der Vertrauenskette installiert sind. Diese Zertifikatskette finden Sie im DFN-PKI-Portal.

Bei Fragen & Problemen

Bei Fragen und Problemen können Sie sich an unseren Helpdesk wenden: **its-helpdesk@ruhr-uni-bochum.de.**

IT.SERVICES | Stand: 15.03.2018