Nutzerzertifikate

1. Zertifikate beantragen

WICHTIG:

- Bei der Zertifikatsbeantragung wird eine Antragsdatei in Form einer .JSON-Datei erzeugt, welche u.a. ihren privaten Schlüssel enthält (siehe Punkt 5). Diese Datei und das zugehörige Passwort sind unbedingt notwendig, um das fertige Zertifikat zu erstellen. Eine verlorene Datei oder ein vergessenes Passwort kann nicht wiederhergestellt werden, was eine neue Beantragung des Zertifikats zur Folge hat.
- Bei der Identitätsfeststellung bitte unbedingt einen gültigen Ausweis (Reisepass oder Personalausweis) verwenden.
- Wenn Sie eine Alias Adresse eingerichtet haben, teilen Sie dies bitte den Mitarbeitern der CA unbedingt mit, da man diese Adressen dann zum Zertifikatsantrag hinzufügen kann.

Im Folgenden finden Sie den Link zur Webschnittstelle der DFN-PKI und eine kurze Anleitung:

Webseite der DFN-PKI:

https://pki.pca.dfn.de/dfn-ca-global-g2/cgi-bin/pub/pki?cmd=getStaticPage&name=index&RA_ID=4150

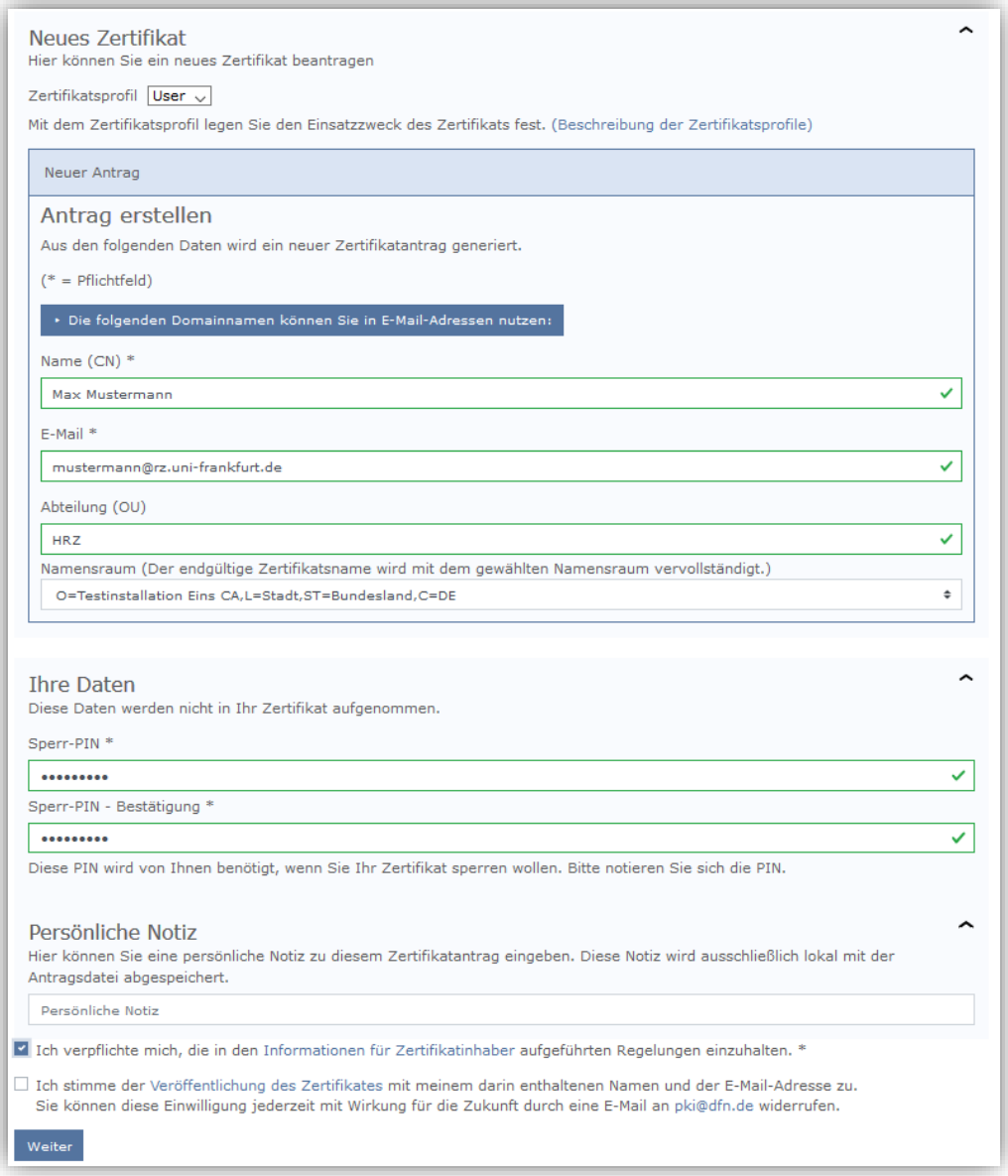
HINWEISE:

- Die erstellte Antragsdatei und das dazugehörige Passwort müssen gut verwahrt werden
- Email-Adresse: Bitte achten Sie darauf, dass Sie ein Zertifikat für die E-Mail-Adresse beantragt, mit der Sie Email versenden.
- Abteilung: Das Eintragen einer Abteilung ist notwendig, bitte tragen Sie daher ihre Abteilung ein. Dies kann ihre Arbeitsgruppe oder die Übergeordnete Abteilung sein.
- Veröffentlichung des Zertifikates: Wenn Sie der Veröffentlichung Ihres Nutzerzertifikats zustimmen, wird dieses zum Verzeichnisdienst der DFN-PKI hinzugefügt, der im Internet frei zugänglich ist. Der Vorteil einer Veröffentlichung besteht darin, dass jeder, der Ihnen eine verschlüsselte E-Mail senden möchte, dies leicht tun kann, da das entsprechende Zertifikat frei verfügbar ist. Da Nutzerzertifikate den Namen und die E-Mail Adresse des Zertifikatnehmers enthalten, sind diese Daten bei einer Zustimmung zur Veröffentlichung frei verfügbar. WICHTIG: Hier wird nicht der Private sondern nur der öffentliche Schlüssel veröffentlicht, welcher auch beim Signieren von E-Mail mitgesendet wird.

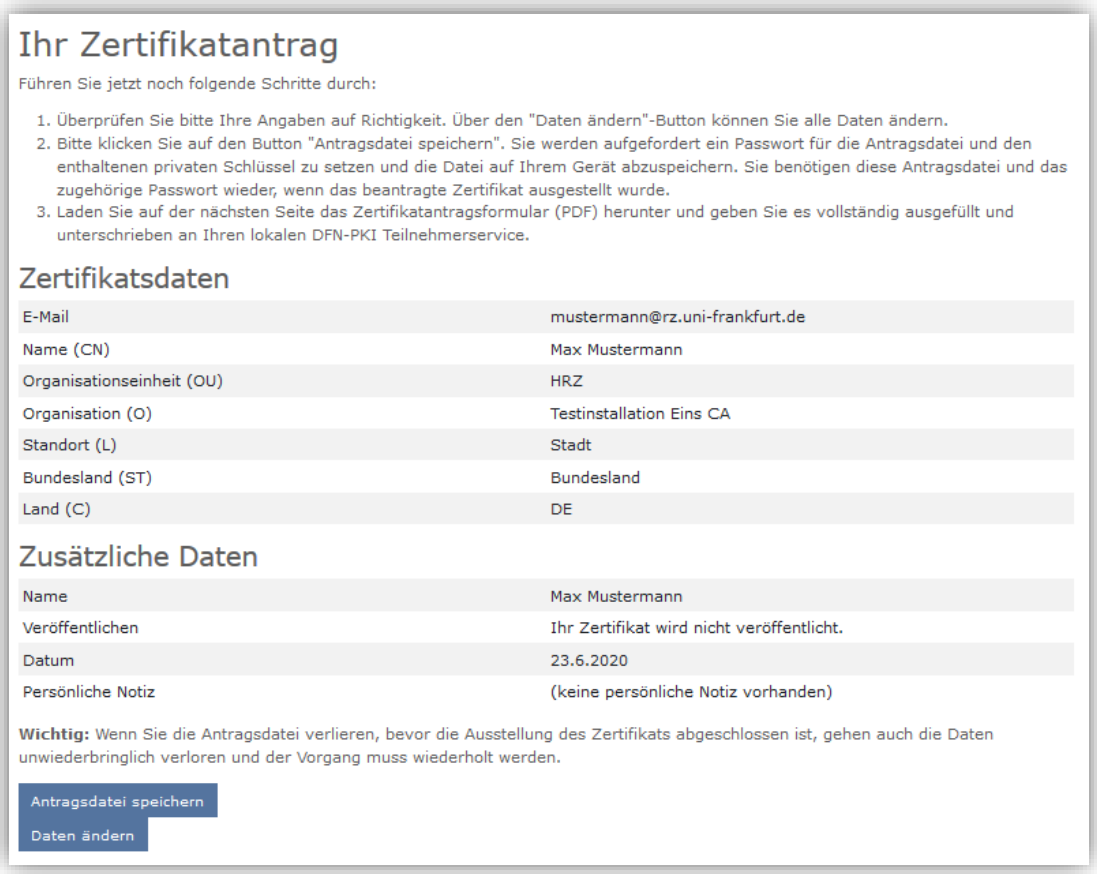
Anleitung:

1. Öffnen Sie den oben stehen Link zur DFN-PKI Webseite.
2. Klicken Sie unter Nutzerzertifikate auf den dort hinterlegten Link. Die Webseiten der DFN-PKI werden gerade umgebaut, daher die Hinterlegung eines zusätzlichen Links.
3. Klicken Sie nun auf „Ein neues Nutzerzertifikat beantragen“

4. Hier müssen Sie nun das Webformular ausfüllen und anschließend auf weiter klicken. Beim Namensraum bitte den Längeren der beiden Einträge (mit den Attributen O, L, ST und C) zu wählen.



5. Im Anschluss erscheint eine Übersichtsseite mit den Zertifikatsinformationen. Überprüfen Sie ihre Daten und klicken Sie anschließend auf „Antragsdatei speichern“ und geben Sie in dem automatisch öffnenden Fenster ein Passwort zur Verschlüsslung der Antragsdatei ein. Die Antragsdatei (.json) enthält auch ihren persönlichen Schlüssel, sollte sie oder das gesetzte Passwort verloren gehen, muss ein neuer Antrag gestellt werden.



6. Anschließend erscheint der Punkt „Zertifikatsantragsformular (PDF) herunterladen“. Laden Sie sich den Antrag herunter, drucken sie Diesen aus und unterschreiben Sie ihn.

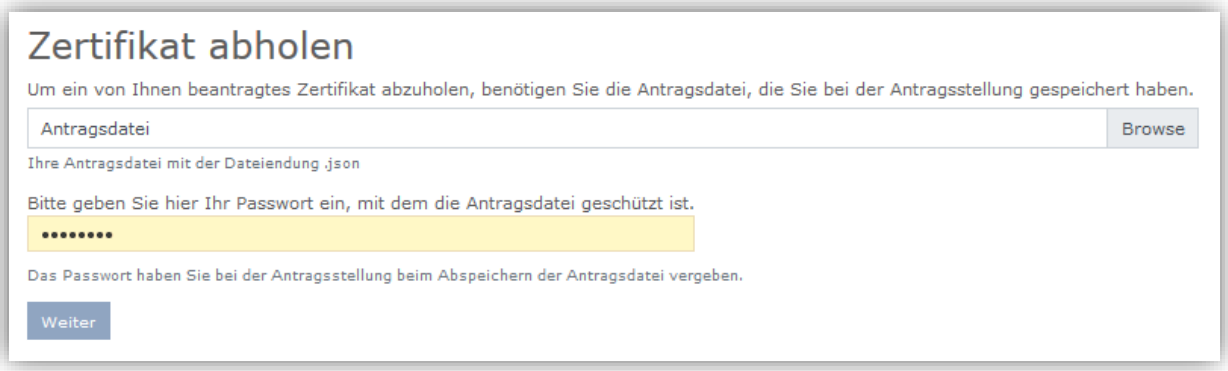
7. Identitätsfeststellung:
    1. Video-Ident Verfahren: Bei diesen Verfahren wird ihre Identität in einer Video-Konferenz verifiziert und die Echtheit des Ausweisdokuments überprüft. Schicken Sie den Scan des unterschriebenen Antrages per Mail an ca@uni-frankfurt.de und geben sie an mit welchen Ausweisdokument Sie sich identifizieren lassen möchten. Die Kollegen der CA melden sich dann bzgl. eines Termins bei Ihnen.
    2. Persönlicher Termin: Mit dem unterschriebenen Antrag, einem gültigen Ausweis (Reisepass oder Personalausweis) zur Identitätsüberprüfung bei den Kollegen des Goethe Card-Service vorbeikommen
8. Nach Genehmigung des Antrags erhalten Sie eine E-Mail vom DFN. Das Zertifikat können Sie dann wie im folgenden Abschnitt „2. Zertifikat herunterladen“ downloaden

2. Zertifikate herunterladen

Genehmigte Zertifikate können im Browser direkt als verschlüsselte p12-Datei heruntergeladen werden.

Anleitung:

1. Öffnen Sie den oben stehen Link zur DFN-PKI Webseite.
2. Klicken Sie unter Nutzerzertifikate auf den dort hinterlegten Link. Die Webseiten der DFN-PKI werden gerade umgebaut, daher die Hinterlegung eines zusätzlichen Links.
3. Klicken Sie nun auf „Ein beantragtes Zertifikat abholen“
4. Im nächsten Fenster klicken sie bitte auf „Browse“, wählen sie ihre Antragsdatei aus und geben Sie nun das zuvor festgelegt Passwort ein.



5. Anschließend werden Ihnen die Zertifikatsinformationen noch einmal angezeigt. Klicken Sie nun bitte auf „Zertifikatsdatei speichern“ und legen Sie ein Passwort für die verschlüsselte p12-Datei fest. Das Passwort benötigen Sie um das Zertifikat in ihren E-Mail Client zu installieren.

    Das IT-Sicherheitsteam empfiehlt Ihnen ein Kennwort von mindestens 16 Zeichen zu wählen, um einen möglichen Identitätsmissbrauch beim Verlust oder Diebstahl vermeiden zu können.

3. Zertifikate im E-Mail Client installieren

Webmail (Horde)

Unter Benutzereinstellungen -> Webmail -> S/MIME die Option „S/MIME-Funktionen“ aktivieren. Das Zertifikat importieren unter Einstellungen -> Benutzereinstellungen -> Webmail -> Allgemeines -> S/MIME -> Ihr persönliches S/MIME-Zertifikat. Wählen Sie das zuvor aus dem Browser exportierte Zertifikat aus und geben Sie Ihr Kennwort ein.

Standardmäßig Signieren unter Einstellungen -> Benutzereinstellungen -> Webmail -> Neue Nachricht -> Erstellen -> Ihre Standard-Verschlüsselungsmethode beim Verschicken von Nachrichten: Unterzeichnen (S/MIME).

Microsoft Outlook:

Zertifikat importieren unter Datei -> Optionen -> Trust Center -> Einstellungen für das Trust Center -> E-Mail Sicherheit -> Digitale IDs(Zertifikate) -> Importieren/Exportieren -> Importdatei. Wählen Sie das zuvor aus dem Browser exportierte Zertifikat aus und geben Sie Ihr Kennwort ein.

Standardmäßig Signieren unter Datei -> Optionen -> Trust Center -> Einstellungen für das Trust Center -> E-Mail Sicherheit -> Verschlüsselte E-Mail-Nachrichten. Setzen Sie ein Häkchen bei "Ausgehenden Nachrichten digitale Signatur hinzufügen" und wählen Sie unter Standardeinstellungen -> Einstellungen -> das importierte Zertifikat aus.

Mozilla Thunderbird:

Zertifikat importieren unter Extras -> Einstellungen -> Erweitert -> Zertifikate -> Zertifikate verwalten -> Importieren… Wählen Sie das zuvor aus dem Browser exportierte Zertifikat aus und geben Sie Ihr Kennwort ein.

Standardmäßig Signieren unter Extras -> Konten-Einstellungen -> unter Ihrem Konto auf S/MIME-Sicherheit -> Digitale Unterschrift -> Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiben: -> Dort Ihr Zertifikat auswählen und ein Häkchen bei "Nachrichten digital unterschreiben (als Standard)" setzten. Sie sollten unter Verschlüsselung auch schon Ihr Zertifikat eintragen, damit Sie später auch E-Mails verschlüsseln können.

Apple Mail (OS X 10.9):

Im ersten Schritt wird die Schlüsselbundverwaltung unter Mac gestartet. Die Schlüsselbundverwaltung ist unter Programme -> Dienstprogramme zu finden. Im Menü Ablage ist der Untermenüpunkt Objekte importieren... auszuwählen. Wählen Sie das zuvor aus dem Browser exportierte Zertifikat aus und geben Sie Ihr Kennwort ein.

Nach dem Starten von Apple Mail wird eine Nachricht geschrieben, die signiert werden soll. Zum Signieren wird das Signatur-Symbol benutzt. Über die Schaltfläche Senden wird dann die signierte E-Mail verschickt. Zur Verschlüsselung der versendeten E-Mail soll das Schloss-Symbol ausgewählt werden.