Serverzertifikat beantragen

Im Folgenden erfahren Sie, wie Sie ein Serverzertifikat von der Zertifizierungsstelle UNI-FR CA erhalten.
Starten Sie den Web-Browser Ihrer Wahl. Im vorliegenden Beispiel wird Mozilla Firefox verwendet. Das Vorgehen ist bei allen Browsern gleich.

Vorbereitende Arbeiten

Vor der Beantragung eines Server-Zertifikates müssen Sie auf dem Server, für den das Zertifikat erstellt werden soll, einen Certificate Signing Request (CSR) erzeugen.
Wie Sie das bewerkstelligen, können Sie in folgenden Dokumenten nachlesen

- **Ein Server-Zertifikat mit Java Keytool bearbeiten**
- **Ein Server-Zertifikat mit openSSL bearbeiten**

Zu Beginn des CSR-Verfahrens wird ein Schlüsselpaar erzeugt. Der dabei erstellte öffentliche Schlüssel wird zusammen mit den Angaben über die Identität des Servers in den CSR eingebaut. Der CSR muss anschließend bei der Antragstellung an den Uni-FR CA Server übermittelt werden.

Die Identitiät des Servers wird mit Hilfe eines DN (distinguished name) festgelegt, der aus mehreren Elementen zusammengesetzt ist:

Element	Bezeichnung	Bedeutung	Wert	Kommentar	Beispiel (Mailserver des RZ)
C	Country Name	Ländercode	**DE**	Dieser Wert ist obligatorisch (bitte Großbuchstaben)	**DE**
ST	State or Province Name	Bundesland	**Baden-Wuerttemberg**	Dieser Wert ist obligatorisch.	**Baden-Wuerttemberg**
L	Locality Name	Stadt	**Freiburg im Breisgau**	Dieser Wert ist obligatorisch.	**Freiburg im Breisgau**
O	Organization Name	Organisation	**Albert-Ludwigs-Universitaet Freiburg**	Dieser Wert ist obligatorisch	**Albert-Ludwigs-Universitaet Freiburg**
1.OU	Organization Unit Name	Organisationseinheit	(Name der Einrichtung)	Dieser Wert ist optional, sie sollten aber hier den Namen Ihrer Einrichtung angeben	Rechenzentrum
2.OU	Organization Unit Name	Organisationseinheit	(Name der Abteilung o.ä.)	Es können weitere OUs angegeben werden.	Netzwerke
CN	Common Name	Name des Servers	(Internetadresse)	Hier geben Sie die textuelle, nicht die numerische Internetadresse an des Servers an	rz.uni-freiburg.de

Die **rot** eingetragenen Werte müssen wie angegeben übernommen werden.

Der (minimale) eindeutige Name sieht also für unser Beispiel so aus:

```
DN: CN=rz.uni-freiburg.de,OU=Rechenzentrum,O=Albert-Ludwigs-Universitaet
Freiburg,C=DE
```

Außerdem ist eine EMail-Adresse anzugeben, die gültig und funktional (also nicht personengebunden) sein sollte, z.B. des Server-Administrators (Beispiel: postmaster@rz.uni-freiburg.de).

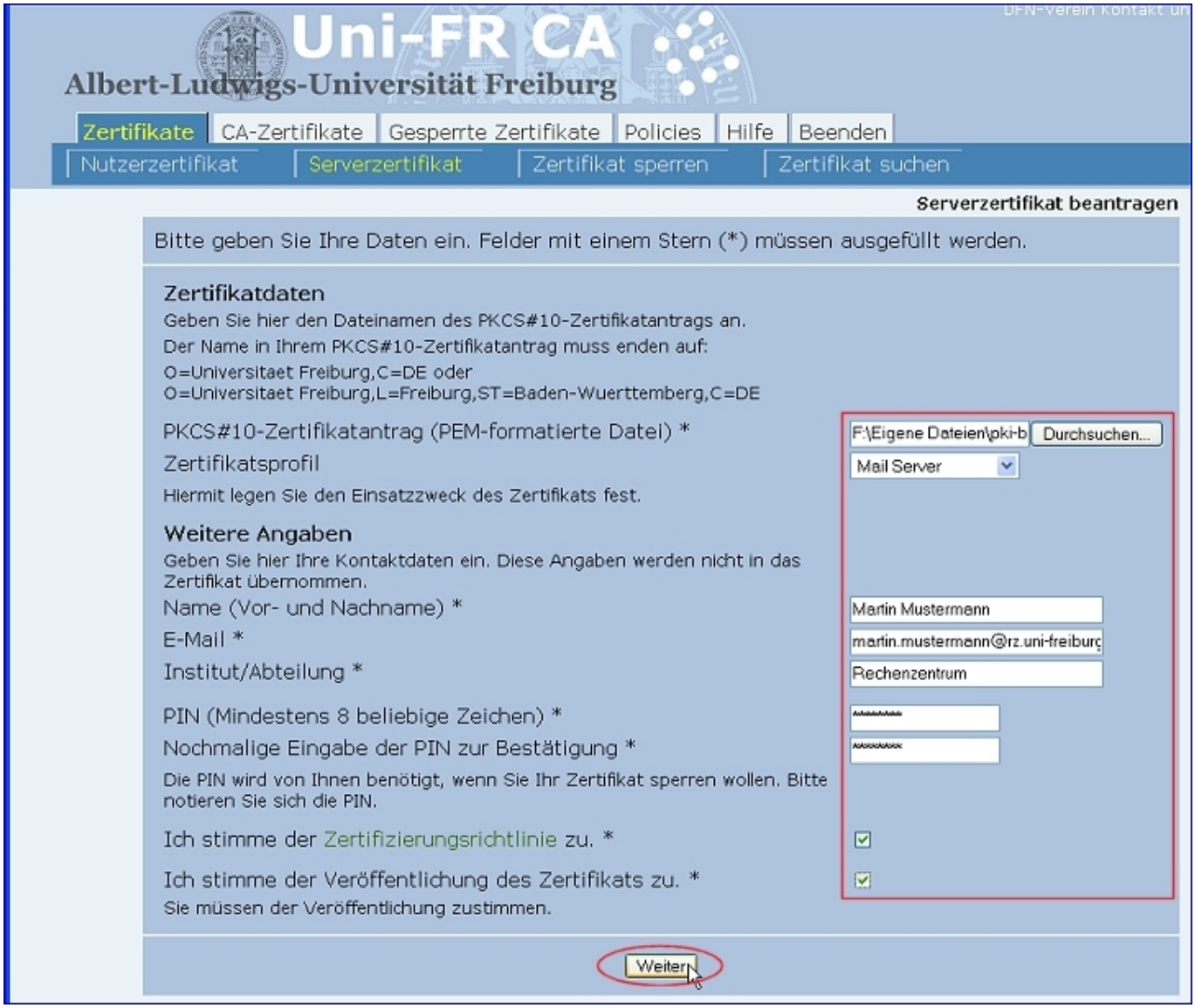
Alle angegebenen Mailadressen müssen existieren.
Es passiert zwar nicht häufig aber mit schöner Regelmäßigkeit, dass die DFN-PKI auf eine ungültige Mailadresse hinweisen muss. Das bedeutet jedesmal manuelles Eingreifen.
Bitte geben Sie also den Antrag erst dann ab, wenn die Mailkonten eingerichtet sind.

Nachdem Sie sich über die Zertifikatsparameter im Klaren sind, rufen Sie die Webseite der Uni-FR CA auf.

Antrag ausfüllen

Als erstes folgen Sie diesem **Link** zur Zertifikatshauptseite der UNI-FR CA.
und klicken Sie auf den Tab „Serverzertifikat“. Füllen Sie nun die Zertifikatsdaten aus. Bitte verwenden sie keine nationalen Sonderzeichen.
NEU: Bitte beachten, geänderte Angaben zu O und ST ab 21.4.2016: O=**Albert-Ludwigs-**Universitaet Freiburg ST=Freiburg **im Breisgau**

Ein Beispiel:



- Zunächst durchsuchen Sie Ihren Speicherplatz nach der abgespeicherten CSR-Datei, die Sie mit Hilfe der Server-Software haben erzeugen lassen. Im Eingabefeld wird der volle Pfadname der Date für den späteren Upload eingetragen.
- Anschließen wählen Sie das Zertifikatsprofil aus.
  Überprüfen Sie ihre Anforderungen mit Hilfe der folgenden Dokumentation:
  https://blog.pki.dfn.de/2016/07/einfuehrung-der-neuen-generation-der-dfn-pki
  Falls Sie kein für Ihre Zwecke dezidiertes Profil finden, wählen Sie das User-Profil.
- Nun folgen die Nutzerangaben mit
  - dem vollem Namen einer Ansprechperson,
  - der Mail-Adresse dieser Ansprechperson,
  - dem Institut oder der Abteilung, die das Zertifikat benötigt und
  - einer (mindestens 8-stelligen) PIN, die zum späteren Verwalten des Zertifikates über die vorliegenden Webschnittstelle benötigt wird.
    (doppelte Eingabe gegen Vertippen)
- Schließlich anerkennen Sie die Zertifizierungsrichtlinien (erforderlich)
  (ein Klick auf den Link unter „Zertifizierungsrichtlinien“ führt Sie zu den Richtliniendokumenten der Uni-FR CA)
  und
- stimmen der Veröffentlichung des Zertifikates zu (erforderlich).

Klicken Sie auf „Weiter“.

Sie sehen im nachfolgenden Fenster noch einmal eine Übersicht der von Ihnen angegebenen Daten, die Sie nun bestätigen oder ändern können. Wenn die Daten korrekt sind, klicken Sie auf „Bestätigen“. Ihr persönlicher Zertifikatsschlüssel wird nun generiert.

Im nächsten Fenster wählen Sie „Zertifikat anzeigen“, um den Zertifikatsantrag als PDF zu betrachten.

DFN-PKI

DFN Deutsches Forschungsnetz

Zertifikatantrag mit Identifizierung

Antragsnummer 36640

...tiger CN=...urg.de, OU=Rechenzentrum, O=Universitaet Freiburg, C=...

...4:19:AC

- Ich ... Identifizierung. ihnen zu.
- Ich stimme der Verarbeitung und Speicherung der bei der Zertifizierung ... werden gemäß den geltenden Datenschutzbestimmungen vertraulich behandelt.

(Ort, Datum) (Unterschrift - wie im Ausweis)

Wird von der Registrierungsstelle ausgefüllt

Prüfung der Ausweisdaten: Bereits geprüft ☐

Name ☐ Unterschrift ☐ Bild ☐ Gültigkeit ☐ Nummer ☐

Name des Prüfers

Zugehörige Registrierungsstelle

(Datum, Unterschrift des Prüfers)

uni-freiburg-ca

Die Registrierungsstelle aufsuchen

Der erste Antrag

Drucken Sie das Antragsformular aus und legen Sie es ausgefüllt persönlich der **Registrierungsstelle** vor.

Die Registrierungsstelle benötigt von Ihnen

- das vollständig ausgefüllte und unterschriebene Antragsformular,
- Ihren gültigen Personalausweis oder Reisepass sowie
- falls Sie nicht Nutzer/Nutzerin des Rechenzentrums sind, ein amtliches Dokument, das Sie als Mitglied der Universität Freiburg ausweist.
  Beispiele: Studierendenausweis, Schriftliche Bescheinigung des Abteilungsleiters.
- eine schriftliche Bestätigung Ihres Institutes, dass Sie zur Verwaltung des angegebenen Servers berechtigt sind.
  (kann selbstverständlich mit der Bestätigung zum vorigen Punkt zusammengefasst werden)

Falls dem Antrag nichts entgegensteht, werden Sie innerhalb weniger Minuten nach der Genehmigung durch die Registrierungsstelle das Zertifikat als Attachement an die persönliche Mailadresse zugeschickt bekommen.

Folgeänträge

Senden Sie das unterschriebene Antragsformular per Hauspost an die RA. Sollte es sich um Serverzertifikate handeln, legen Sie bitte auch eine Bescheinigung der beschäftigenden Einrichtung vor, dass Sie berechtigt sind, die betreffenden Server zu verwalten - sofern dies noch nicht geschehen ist. Beim Postversand wird die Identifizierung des Antragstellers mit Hilfe der Unterschrift durchgeführt.

Es steht Ihnen selbstverständlich frei, nach der Methode des Erstantrages vorzugehen.

Installieren Sie anschließend das Zertifikat an dem dafür bestimmten Ort auf dem Server.

Zertifikate - Artikelübersicht, Sicherheit - Artikelübersicht