Beantragung von Zertifikaten für Server der Universität Passau über den DFN-PKI-Dienst

Serverzertifikate der DFN-PKI müssen im Selfservice-Verfahren direkt über die Web-schnittstelle der DFN-PKI beantragt werden.

Zuvor muss offline ggf. ein privater Schlüssel sowie ein Certificate Signing Request (CSR) erzeugt werden. Dies wird hier am Beispiel der OpenSSL-Software erklärt. Wenn Sie eine andere Software verwenden, konsultieren Sie bitte die Dokumentation Ihrer Software.

1. Erzeugung eines private Key

Dies ist nur notwendig, wenn für den betreffenden Server noch kein entsprechender Key (RSA, mindestens 2048 Bit Länge) vorliegt.

```
openssl genrsa -out <secretkeyfile> <laenge>
```

Hierbei ist <secretkeyfile> der Name der Datei, in die der private Key geschrieben wird, <laenge> die gewünschte Schlüssellänge (mindestens 2048).

2. Erzeugung des CSR

Der Zertifikatsantrag (CSR) muss im PKCS#10-Format als PEM-kodierte Datei vorliegen und kann mit folgendem Kommando erzeugt werden:

```
openssl req -new -key <secretkeyfile> -out <csrfile> \
-subj <subjectstring>
```

<secretkeyfile> ist der Name der Datei, in der sich der private Key bereits befinden muß. <csrfile> ist der Name der Datei, in die der CSR geschrieben wird.

<subjectstring> ist der zu zertifizierende Name in folgendem Format (bitte für das OpenSSL-Kommando in Anführungszeichen einschließen):

/C=DE/ST=Bayern/L=Passau/O=Universitaet Passau/OU=<einrichtungsname>/CN=<servername>

Hierbei sollte für <einrichtungsname> die Bezeichnung der Einrichtung angegeben werden, die den Server betreibt, <servername> ist der Name des Servers als FQDN. <servername> muss auf ".uni-passau.de" enden! Wir behalten uns vor, den Einrichtungnamen zwecks Standardisierung ggf. anzupassen. Die anderen Teile des <subjectstring> dürfen nicht variiert werden.

Bitte beachten Sie, dass Umlaute im <subjectstring> nicht zugelassen sind. Bitte verwenden Sie ggf. die übliche Substitution:
Ä → Ae, Ö → Oe, Ü → Ue, ä → ae, ö → oe, ü → ue, ß → ss.

Wie kann man einen CSR für mehrere FQDNs erzeugen?

Verwenden Sie die OpenSSL-Konfigurationsdatei "uni-passau-req.cnf", die Sie unter folgendem Link downloaden können:

http://www.rz.uni-passau.de/fileadmin/Dateien/Dokumente/Rank/uni-passau-req.cnf

Bitte passen Sie die Einträge für "OU" und "CN" für Ihren Server an. Mit den Einträgen "DNS.2", "DNS.3", ... können Sie weitere FQDNs angeben, für die das Zertifikat gelten soll. Bitte beachten Sie, dass der bei "CN" angegebene Servername unbedingt auch in "DNS.1" angegeben werden muss. Nicht benötigte "DNS."-Einträge löschen Sie bitte.

Den CSR können Sie dann folgendermaßen erzeugen:

```
openssl req -new -key <secretkeyfile> -out <csrfile> \
-config uni-passau-req.cnf
```

3. Online-Beantragung des Zertifikats

Gehen Sie mit einem Webbrowser auf die Seite

http://www.zim.uni-passau.de/dienstleistungen/netzwerk-und-server/server-zertifizierungen/online-antrag/

Sie gelangen dann über einen weiteren Link auf die Einsteigsseite der Nutzerschnittstelle für die Beantragung von Zertifikaten:

Wählen Sie den Punkt "Serverzertifikate":

Bei "PKCS#10-Zertifikatsantrag" ist der Name der in Punkt 2 erzeugten CSR-Datei anzugeben. Mit der Option "Zertifikatsprofil" legen Sie den Typ des Servers fest.

Bitte tragen Sie in die weiteren Felder Ihre Kontaktdaten ein. Der Name muss mit den Angaben in Ihrem Ausweis übereinstimmen. Die E-Mail-Adresse muss eine Adresse

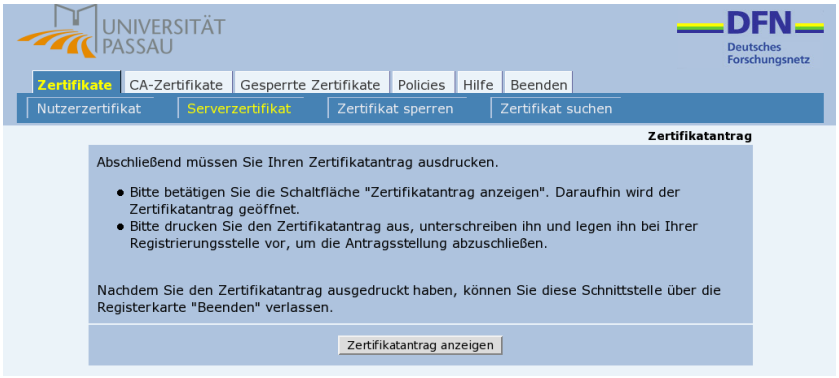
der Universität Passau sein. An diese Adresse wird das erstellte Zertifikat geschickt. Als "Abteilung" geben Sie bitte den Lehrstuhl oder die Einrichtung an, bei der Sie beschäftigt sind.

Für evtl. notwendige Sperrungen eines Zertifikats müssen Sie eine PIN festlegen.

Den einschlägigen Zertifizierungsrichtlinen müssen Sie zustimmen; ob Ihr Zertifikat im Verzeichnisdienst der DFN-PKI veröffentlicht wird, können Sie frei entscheiden.

Nach Klicken auf "Weiter" wird der Antrag nochmals angezeigt:

Wenn die Angaben korrekt sind, können Sie auf "Bestätigen" klicken:



Sie müssen sich nun das automatisch generierte Antragsformular anzeigen lassen. Drucken Sie dieses aus, vervollständigen Sie die Angaben und unterschreiben Sie das Formular. Bitte beachten Sie: Wenn aufgrund unserer Unterlagen die Zugehörigkeit des Antragstellers zur angegebenen Abteilung nicht ersichtlich ist oder der Antragsteller kein Universitätsmitarbeiter ist, muss zusätzlich der Abteilungsleiter den Antrag formlos bestätigen. Dies kann durch einen Vermerk mit Unterschrift und Stempel direkt auf dem Antragsformular geschehen.

4. Persönliche Identifizierung

Das ausgefüllte und unterzeichnete Formular müssen Sie nun im ZIM zusammen mit einem amtlichen Lichtbildausweis nach vorheriger telefonischer Terminvereinbarung zur Identifizierung vorlegen. Bitte wenden Sie sich hierzu an Herrn Eiler (Tel. 1815), Herrn Rank (Tel. 1838) oder Herrn Kornexl (Tel. 1812).

5. Ausstellung des Zertifikats

Nach erfolgter Vornahme der Identifizierung werden unsere Mitarbeiter die Daten im Zertifikatsantrag prüfen, und, wenn keine Rückfragen mehr erforderlich sind, die Ausstellung des Zertifikats veranlassen. Dieses wird Ihnen per E-Mail an die im Antrag angegebene Adresse zugeschickt. I. A. erhalten Sie Ihr Zertifikat spätestens am übernächsten Arbeitstag nach der Identifizierung.

6. Gültigkeitsdauer und Zertifikatsverlängerung

Ein Serverzertifikat gilt für 2 Jahre (genau: 730 Tage) ab Ausstellung. Bitte beantragen Sie vor Ablauf ggf. rechtzeitig ein neues Zertifikat. Eine Verlängerung von Zertifikaten auf der Grundlage eines schon eingereichten Zertifikatsantrags ist leider nicht möglich.

7. Hinweise für die Konfiguration des Apache-Servers

Der erzeugte private Schlüssel und das ausgestellte Zertifikat können mit folgenden Konfigurationsbefehlen im Apache-Server genutzt werden:

```
SSLCertificateFile <certificatefile>
SSLCertificateKeyFile <secretkeyfile>
```

Hierbei ist <certificatefile> der vollständige Pfad zu der von der DFN-PKI gelieferten Zertifikatsdatei, <secretkeyfile> ist der vollständige Pfad zu der unter 1. erzeugten Datei mit dem private Key. Achten Sie darauf, die Zugriffsrecht auf letztere Datei so zu setzen, dass nur der Apache-Webserver Zugriff auf die Datei hat.

Damit ein Webbrowser die von der DFN-PKI ausgestellten Zertifikate wirklich bis zu einer Stammzertifizierungsstelle zurückverfolgen kann, die im Browser bereits als vertrauenswürdig vorinstalliert ist, empfiehlt es sich, die Zertifikatskette in der Apache-Serverkonfiguration zu spezifizieren. Dies geht mit dem Konfigurationsbefehl

```
SSLCertificateChainFile <certificatechainfile>
```

Die Datei <certificatechainfile> können Sie von der Webschnittstelle der DFN-PKI folgendermaßen downloaden: Gehen Sie mit einem Webbrowser auf die Einstiegsseite der Nutzerschnittstelle (siehe Punkt 3.). Klicken Sie dort auf "CA-Zertifikate". Klicken Sie dann (zum Download bei den meisten Browsern mit der rechten Maustaste) auf "Zertifikatkette anzeigen". Sie können dann die Datei als <certificatechainfile> abspeichern.