Einen CSR-Requests für ein Serverzertifikat mit Java Keytool erstellen

Auf dieser Seite zeigen wir Ihnen, wie Sie mit Java Keytool ein Schlüsselpaar generieren, den CSR erzeugen und schließlich das von der Uni-FR CA gelieferte Zertifikat in das Server-System einbauen.

Schlüsselpaar generieren

Im vorliegenden Beispiel wollen wir folgendes voraussetzen:

- Die Internet-Adresse des Servers sei **server1.ruf.uni-freiburg.de**
- Die Abteilung ist das **Rechenzentum**
- Der Schlüsselbund zur Aufbewahrung der eigenen Schlüssel sei **/var/lib/.keystore** (unter Windows üblicherweise C:\Dokumente und Einstellungen\(Benutzername)\.keystore)
- Der Schlüssel soll auf hohe Sicherheit (Länge **2048 Bit**) eingestellt sein
- Der Gültigkeitszeitraum wird auf die maximale von der Uni-FR CA akzeptierten Zeitdauer von 1 Jahr und 1 Monat konfiguriert

Es soll hier ein Schlüsselpaar inclusive einem selbstsignierten Zertifikat mit folgendem eindeutigen Name erzeugt werden:

```
DN: CN=server1.ruf.uni-freiburg.de,OU=Rechenzentrum,O=Albert-Ludwigs-
Universitaet Freiburg,L=Freiburg im Breisgau,ST=Baden-Wuerttemberg,C=DE
```

Für die Uni-FR CA sind die Komponenten O und C obligatorisch: **O=Albert-Ludwigs-Universitaet Freiburg,L=Freiburg im Breisgau,ST=Baden-Wuerttemberg,C=DE**.
Das Element OU kann auch mehrfach auftreten, falls Sie z.B. verschiedene Unterabteilungen im DN nicht nur durch den CN des Servers kenntlich machen wollen.

Das Java Keytool Kommando zur Herstellung eines Schlüsselpaares lautet folgendermaßen:
(Die Benutzer-Eingabezeilen sind in den Beispielen mit dem System-Promp '>' gekennzeichnet)

```
> keytool -genkey -alias mykey -keyalg RSA -keysize 2048 -validity 1825
     -keystore /var/lib/.keystore
     -dname "CN=server1.ruf.uni-freiburg.de,OU=Rechenzentrum,O=Albert-
Ludwigs-Universitaet Freiburg,L=Freiburg im Breisgau,ST=Baden-
Wuerttemberg,C=DE"
```

Die Zeilenumbrüche sind hier nur der Übersichtlichkeit halber eingesetzt. Bitte geben Sie das Kommando komplett in einer Zeile ein!

Sie werden nach einem Keystore-Passwort gefragt, mit dem die Keystore-Datei gegen unbefugten Zugriff geschützt werden soll. Die Anwendungen, die diese Schlüssel nutzen, müssen in der Lage sein, dieses Passwort beim Start bereitzustellen. Dabei sollten Sie peinlich darauf achten, dass dieses Passwort keinem Unbefugten zugänglich ist.

Weiterhin werden Sie nach einem Passwort für den Keystore-Eintrag (hier alias=mykey) gefragt, das den Zugang zum privaten Schlüssel dieses Eintrages schützt. Es kann identisch zum Keystore-Passwort gewählt werden.

Das Schlüsselpaar liegt nun unter dem Alias-Namen „mykey“ eingepackt in ein selbstsigniertes X.509-Zertifikat im Schlüsselbund vor. Es ist dringend zu empfehlen, von dieser Datei eine Sicherungskopie zu erstellen.

Zertifizierungsantrag generieren

Nun soll aus den Angaben im Schlüsselbund ein CSR erstellt werden. Dazu lautet das Kommando:

```
> keytool -certreq -alias mykey -keyalg RSA -file server1.csr -keystore
/var/lib/.keystore
```

Damit erzeugen Sie für den Schlüsselbund-Eintrag „mykey“ die Request-Datei unter dem Namen server1.csr

Internes