Serverzertifikat mit Java Keytool bearbeiten

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.

Hintergrundinformationen dazu finden Sie in dem Dokument **Ein Serverzertifikat beantragen**.

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.

Diese Datei können Sie im Web-Interface der Uni-FR CA

Link

direkt über die Schaltfläche Durchsuchen hochladen lassen.

Das Antragsverfahren mit Hilfe des Web-Interface der Uni-FR CA ist beschrieben in dem Dokument

- **Serverzertifikat beantragen**

Zertifikat und privaten Schlüssel installieren

Sobald Sie das Serverzertifikat von der Uni-FR CA per Mail erhalten haben, speichern Sie die PEM-formatierte Datei des Attachements ab, z.B. unter dem Namen **server1.pem**.

Außerdem speichern Sie das **Zertifikat der Wurzelzertifizierungsstelle** der Deutschen Telekom, das **Zwischenzertifikat der DFN-PKI** sowie das **Zertifikat der Uni-FR CA** als PEM-Datei ab. Klicken Sie dazu mit der rechten Maustaste auf die Links und wählen Sie die Funktion „Ziel speichern unter…“. Die heruntergeladenen Dateien werden gespeichert unter den Namen **g_deutsche-telekom-root-ca-2.pem**, **g_dfn_intermediatecert.pem** bzw. **g_unifrcacert.pem**.

Als erstes importieren Sie die drei Zertifikate der Zertifikatskette in die keystore-Datei:

```
> keytool -import -file g_deutsche-telekom-root-ca-2.pem -alias root -
keystore /var/lib/.keystore
> keytool -import -file g_dfn_intermediatecert.pem -alias dfn -keystore
/var/lib/.keystore
```

```
> keytool -import -file g_unifrcacert.pem -alias unifrca -keystore
/var/lib/.keystore
```

Das Wurzelzertifikat muss manuell von Ihnen als vertrauenswürdig eingestuft werden. Es ist deshalb gute Praxis, wenn Sie grundsätzlich den **Fingerabdruck** der Zertifikatsdatei mit dem auf der Download-Seite vergleichen. Die weiteren Zertifikate werden auf Grund der schon importierten Zertifikate von der Software als vertrauenswürdig erkannt.

Geben Sie den Zertifikaten sprechende Aliasnamen, damit man sie leicht wiederfinden kann und halten Sie die angegebene Reihenfolge beim Import ein!

Anschließend importieren Sie das per Mail erhaltene Zertifikat in Ihre Keystore-Datei.
Geben Sie dabei den bei der Schlüsselerstellung verwendeten Aliasnamen an:

```
> keytool -import -file server1.pem -alias mykey -keystore
/var/lib/.keystore
```

Keytool stellt dabei eine sog. Vertrauenskette vom server1-Zertifikat über das Uni-FR CA Zertifikat bis zum selbstsignierten root-Zertifikat her und legt sie unter dem Aliasnamen server1 ab.

Konfigurieren Sie nun die Serverdienste, die auf das Zertifikat zugreifen sollen, entsprechend der individuellen Dokumentation. Normalerweise müssen Sie die Anwendungen anschließend neu starten, damit die Konfiguration wirksam wird und das Zertifikat verwendet werden kann.

Wie Sie die Zertifikate am Beispiel von Tomcat nach den Vorgaben von Apache HTTPD bereitstellen können, zeigt das Beispiel auf der Seite **"Serverzertifikat mit openSSL bearbeiten"**

Zertifikate - Artikelübersicht, Sicherheit - Artikelübersicht, Artikel zum tag: keytool