

Update der bmiKundenCA-Zertifikate

... inklusive der Test-Zertifikate aus der bmiKundenTestCA

(Stand 2004-03-17, [St. Patrick](#) ;-) (Korrekturen in JAVA-Anleitung: 2004-03-18)

Warum .pem, .der und nicht .jks und .p12?

Die ursprünglichen Dateien, jks, und pkcs#12, enthielten die Schlüssel (– speziell den hochsensiblen „private key“, der nicht in fremde Hände gelangen darf).

Der derzeit notwendige Update betrifft nur das Zertifikat, das letztlich die Gültigkeit der Schlüssel und damit die Identität des Schlüsselinhabers bestätigt.

Die Details:

Bei diesem Zertifikat handelt es sich um ein Dokument, das den öffentlichen Schlüssel (den jeder sehen darf) von Ihnen enthält, zusammen mit Daten, die den Zertifikatsbesitzer beschreiben. Dieses Dokument wird dadurch zu einem Zertifikat, dass es von der bmiKundenCA, bzw. bmiKundenTestCA unterschrieben ist.

(Digital signiert: Über den Inhalt des Dokuments wird ein hash gebildet, der mit dem CA-Schlüssel verschlüsselt wird. Jeder, der Zugriff auf den öffentlichen Schlüssel der CA hat, der im Wurzelzertifikat der CA enthalten ist, kann dadurch die Gültigkeit aller Zertifikate überprüfen, die von dieser CA signiert wurden.)

Dieses Zertifikatsdokument wird jeweils mit einer beschränkten Gültigkeitsdauer ausgestellt und muss daher regelmäßig erneuert werden.

Was sind die notwendigen Schritte, des Zertifikatsupdates?

Da die Wurzel-Zertifikate, die mit Ihrem Kundenzertifikat mitgeliefert wurden, bereits abgelaufen sind, sollten Sie auch diese neu installieren.

Bevor Sie Änderungen am laufenden System durchführen, sollten Sie jedenfalls ein **Backup** der Keystores (Schlüsselspeicher, die auch die Zertifikate enthalten) durchführen.

Wurzel-Zertifikate erneuern (Root Certificates)

Die Zertifikate bmiKdCAcert.* und bmiKdTestCAcert.* müssen unter „trusted root certificates“ also „vertrauenswürdige Aussteller-Zertifikate“, installiert werden.

Bei den **verschiedenen Zertifikats-Management Lösungen** (IBM iKeyman, MS CCM, ...) gibt es eine eigene Kategorie, die so oder ähnlich heißt. In dieser Kategorie sind auch die Ausstellerzertifikate von Verisign, Thawte und anderen enthalten.

Diesen Schritt haben Sie bereits bei der Erstinstallation einmal durchgeführt, es sei denn Sie verwenden Java-Keystores:

Unter Java gibt es die Datei \$JAVA_HOME/jre/lib/security/cacerts, in der die Trusted Certificates gespeichert werden (Pfad kann in Versionen etwas variieren!).

Mit nachfolgendem Befehl wird ein Root-Cert importiert (... Pfad anpassen, ggf. anderes Passwort, Backslash auslassen, signalisiert nur Zeilenumbruch!).

```
keytool -import -alias bmiKdCA -file bmiKdCAcert.der \  
-keystore $JAVA_HOME/jre/lib/security/cacerts -storepass  
changeit
```

Das Ganze nochmals für das bmiKdTestCAcert!

Das eigene Zertifikat aus der Serie 5-000-0xx erneuern

Jeweils eine der beiden gleichlautenden Dateien mit der unterschiedlichen Endung *.der und *.pem wird in das passende Keystore eingespielt.

Bei den **verschiedenen Zertifikats-Management Lösungen** (IBM iKeyman, MS CCM, ...) wird in der Kategorie „Eigene Zertifikate“ das *.pem oder *.der importiert.

Unter Java haben Sie das ursprüngliche Keystore, *.jks, an geeigneter Stelle in Ihrem System abgelegt. In diesem jks ist das Zertifikat mit einem Alias verknüpft abgelegt. Ein Update geschieht dadurch, dass zu diesem Alias ein neues Zertifikat importiert wird. Wichtig ist dabei, dass das Alias für den Schlüssel und für das Zertifikat zusammenpassen.

Um den Alias herauszufinden, verwenden Sie bitte folgenden Befehl:

```
keytool -list -keystore 5-000-999-pj.jks \  
-storepass xyzabcdef
```

Keystore-Name und Passwort anpassen!

Unter dem entsprechenden Alias können Sie dann das neue Zertifikat einspielen:

```
keytool -import -alias bmiKdCA_5-000-999-pj \  
-file 5-000-999-pj-1.der -keystore 5-000-999-pj.jks \  
-storepass xyzabcdef -trustcacerts
```

(Name, Pfad und Passwort anpassen!)

Sollte Ihre Umgebung mit diesen Lösungsansätzen nicht zurechtkommen, bitte unter „Zertifikatserneuerung zu Fuß“ weiterlesen!

Testen

Nachdem Sie diese Arbeitsschritte durchgeführt haben, sollte Ihr System wie gewohnt auf das BMI-Portal zugreifen können.

Nur im Problemfall: Zertifikatserneuerung zu Fuß

Dazu benötigen Sie das ursprüngliche pkcs#12 File und OpenSSL.

OpenSSL ist Standard unter Unix und Linux. Unter Windows kann man OpenSSL ebenso verwenden, Details unter <http://www.iconsinc.com/~agray/openssldev/> beziehungsweise <http://www.openssl.org>.

Sinngemäß lässt sich der gleiche Vorgang auch mit anderen Hilfsmitteln bewerkstelligen, die pkcs#12 Stores verarbeiten können.

Aus dem ursprünglichen pkcs#12 exportieren Sie die Inhalte in ein Text-File:

```
openssl pkcs12 -in 5-000-0xx-pp.p12 -out allof_5-000-0xx-pp.txt
```

Dabei werden Sie nach dem Keystore-Passwort und dem Import-Passwort (2x) gefragt. Verwenden Sie das ursprünglich mit dem Keystore verbundene Passwort.

Aus der Textdatei, die Sie im ersten Schritt erzeugt haben, kopieren Sie nun die Zeilen von

```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: DES-EDE3-CBC,...
```

bis

```
-----END RSA PRIVATE KEY-----
```

in eine neue Datei, z.B. meinSchluessel.key.pem, in Ihr Arbeitsverzeichnis.

Stellen Sie in dieses Verzeichnis auch die passende neue .pem-Datei, also etwa 5-000-0xx-pp-1.cert.pem

Anschließend führen Sie aus:

```
openssl pkcs12 -export -name bmiKdCA_5-000-0xx-pp \  
-in 5-000-0xx-pp-1.cert.pem -inkey meinSchluessel.key.pem \  
-passin pass:xyzabcdef -passout pass:xyzabcdef \  
-out neu-5-000-0xx-pp.p12
```

(Passwort, Filename anpassen!)

Damit haben Sie eine installierbare Version eines erneuerten pkcs#12, (=*.p12), die genauso installiert werden kann, wie bei der Erstinstallation.

Viel Erfolg!