TeleSec ServerPass

Java Keytool Requesterzeugung

Version: 2.9a
Stand: 10.09.2014
Status: Final

Impressum

Herausgeber
T-Systems International GmbH GCU Midmarket Public Health & Security, PSS - Trust Center Solutions Untere Industriestraße 20 57250 Netphen

Dateiname	Dokumentennummer	Dokumentenbezeichnung
serverpass_req_inst_java_keytool 2 9a.doc		Requesterzeugung Java Keytool

Version	Stand	Status
2.9a	10.09.2014	Final

Autor	Inhaltlich geprüft von	Freigegeben von
T-Systems International GmbH GCU Midmarket Public Health & Security, PSS - Trust Center Solutions	W. Bohn	L. Eickholt

Ansprechpartner	Telefon / Fax	E-Mail
Servicedesk	Telefon: +49 (0) 1805 268 204 * * Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute	Telesec_Support@t-systems.com

Kurzinfo
Java Keytool Requesterzeugung

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	01.01.2003	Trust Center T-Systems, ASC	Erster Entwurf
1.0	01.04.2004	Trust Center T-Systems, ASC	Inhalt- und Layoutanpassung
1.1	22.05.2005	Trust Center T-Systems, ASC	Layoutanpassung
1.2	22.08.2006	Trust Center T-Systems, ASC	Inhalt- und Layoutanpassung
1.3	26.03.2010	Trust Center T-Systems, ASC	Inhaltliche Anpassung
2.0	30.04.2010	W. Bohn	Inhalt- und Layoutanpassung
2.1	01.06.2010	W. Bohn	Inhaltliche Anpassung
2.2	16.06.2010	W. Bohn	Inhaltliche Anpassung
2.3	05.10.2010	W. Bohn	Inhaltliche Anpassung
2.4	07.01.2011	W. Bohn	Inhaltliche Anpassung
2.5	20.01.2011	W. Bohn	Inhaltliche Anpassung
2.6	27.01.2011	W. Bohn	Inhaltliche Anpassung
2.7.	09.02.2011	W. Bohn	Inhaltliche Anpassung
2.8	11.02.2013	W. Bohn	Inhaltliche Anpassung
2.9	10.04.2014	M. Burkard	Anpassung der Links
2.9a	10.09.2014	W. Bohn	Inhaltliche Anpassung

Inhaltsverzeichnis

1 Allgemeines

Dieses Dokument beschreibt die Requesterzeugung sowie die Einbindung der Zertifikate im Java Keytool.

Bitte lesen Sie zuerst folgende Hinweise!

Sichern Sie Ihre Daten! Die Verwendung dieser Anleitung wurde hinreichend getestet. Jedoch kann für den unwahrscheinlichen Fall eines Datenverlustes keine Haftung übernommen werden.

Dieses Dokument beinhaltet eine **Anleitung zur Erzeugung eines Server-Zertifikat-Requests sowie dem Import der Zertifikate mittels Java keytool für Java basierende Webserver, die auf einen Java Keystore zugreifen.**

Weiterführende Erklärungen über den Einsatz von SSL-Zertifikaten zur Absicherung des Webservers entnehmen Sie bitte der Dokumentation des Webservers.

Bitte verwenden Sie für die Bearbeitung der Request- und Zertifikatsdateien einen möglichst einfachen Editor, zum Beispiel „vi“ unter Linux/Unix bzw. „MS-Editor oder „Wordpad“ unter Windows.
Wenn Sie Wordpad einsetzen, verwenden Sie stets die Option „Als Textdokument abspeichern“.

Editoren aus Officepaketen können den Inhalt der Request- und Zertifikats-Dateien verfälschen und damit unbrauchbar machen.
Weiterhin beachten Sie bitte die in der CPS (**C**ertificate **P**ractice **S**tatement) gemachten Angaben bzgl. des erlaubten Zeichensatzes.

Weitere Informationen und Tipps erhalten Sie auf unserer Internetseite im „FAQ-Bereich“.

Siehe hierzu: https://www.telesec.de → ServerPass → Support

Hier gezeigt wird die Beauftragung eines ServerPass unter Verwendung des Produkts „ServerPass Standard“.

Da für die Ausstellung der Server-Zertifikate unterschiedliche CA-Zertifikate zum Einsatz kommen können, ist auf die Verwendung der korrekten CA-Zertifikate im Webserver zu achten!

Die herunter geladene Datei „Download (incl. Zertifikatskette)“ enthält stets die zusammengehörigen User-, CA-, und Root-Zertifikate. Verwenden Sie bitte das CA-Zertifikat und wenn gewünscht, auch das Root-Zertifikat aus der herunter geladenen Datei.

Alternativ lassen sich alle CA- und Root-Zertifikate lassen sich auf unserer Internetseite herunterladen.

Siehe hierzu: https://www.telesec.de → ServerPass → Support → Root- / Sub-CA-Zertifikate

Hier werden ebenfalls alle relevanten Details wie Seriennummer, Laufzeit, Fingerprints usw. der einzelnen Zertifikate angegeben.

Für die hier gezeigten Befehle und Konfigurationsänderungen sind in der Regel „Administrator-„ oder „root-“ bzw. „sudo-Rechte erforderlich“.

Bitte beachten Sie:
ein Request kann nur für die Beauftragung eines Zertifikats bzw. für die Beauftragung einer Zertifikatserneuerung verwendet werden.

Wird der gleiche „Public Key“ mehrfach für eine Beauftragung eingereicht, so werden die weiteren Beauftragungen abgewiesen.

Möchten Sie für den gleichen Webserver mehrere Zertifikate beauftragen (z. B. zuerst ein Testzertifikat und anschließend ein Wirkzertifikat), so erzeugen Sie zunächst einen Request, wie in dieser Anleitung beschrieben. Soll das Zertifikat zu einem späteren Zeitpunkt durch ein anderes ersetzt werden, so muss im Server ein neuer Schlüssel und somit ein neuer Request erzeugt werden.

1.1 Testzertifikate

Testzertifikate werden ebenfalls angeboten.

Nachdem Sie sich im Kundenportal „myServerPass“ angemeldet haben, gelangen Sie über die Produktauswahl „TeleSec ServerPass Test“ zum Beauftragungsformular von Testzertifikaten.

Die hierbei verwendeten ausstellenden Instanzen (Root- und CA-Zertifikate) sind in keinem Server- oder Client-Produkt verankert. Für einen erfolgreichen Testablauf ist ggf. die Installation aller ausstellen Instanzen sowohl im Server- als auch in der Client- Produkt erforderlich.

Die Laufzeit der ausgestellten Testzertifikate ist auf 30 Tage beschränkt.

Die Beauftragung und Installation der Zertifikate verläuft analog zum hier gezeigten.

1.2 Spezielle Hinweise für Java Keytool

Die Beschreibung bezieht sich auf folgende Softwarekonstellation:

Java: 1.7.0_11-b21 (deutsch)
Plattform: Plattformübergreifend (hier gezeigt wird die Vorgehensweise in einer Windows-Umgebung)

Voraussetzung: Alle Komponenten für Java wurden korrekt installiert.

Es wird das von Java bereitgestellte Programm „keytool“ verwendet.
Die Aufrufe erfolgen jeweils aus einer Windows Eingabeaufforderung (CMD) bzw. unter einer Konsole unter Linux/Unix. Das Programm keytool bietet eine Vielzahl an Optionen und Möglichkeiten. Einen Überblick hierüber bietet der Aufruf von: **keytool.exe -help**

2 Keystore- , Schlüssel und Requesterzeugung, Beauftragung, Installation, Sicherung der Dateien

2.1 Erzeugung einer Keystore-Datei

Die während der Schlüsselerzeugung gemachten Angaben sind unveränderbar und erscheinen später im Schlüssel sowie im Zertifikat.

Während der Schlüsselerzeugung sind folgende Angaben erforderlich:

alias(*)	z. B.	testhost.example.com	Alias für den Schlüssel
keystore	z. B.	keystorefile	Name für die Keystore-Datei
storepass	z. B.	keystorepassword	Passwort für die Keystore-Datei, ein späterer Zugriff auf die Keystore-Datei ist nur mit diesem Passwort möglich, Standard: changeit
keypass	z. B.	keypassword	Passwort für den Schlüssel, ein späterer Zugriff auf den Schlüssel ist nur mit diesem Passwort möglich, Standard: changeit

keysize	Die Zahl nach Keysize legt die die verwendete Bitlänge (Schlüssellänge) des Server-Keys und der späteren Zertifikate fest. Mögliche Werte sind: 2048 oder 4096 Empfohlen wird eine Bitlänge von 2048, maximal jedoch 4096 Bit. Requests mit einer Bitlänge kleiner 2048 Bit gelten nicht länger als sicher und sind von der Beauftragung ausgeschlossen.
keyalg	Schlüssel Algorithmus. Dieser Wert muss als **RSA** definiert sein. Andere Algorithmen werden aktuell nicht unterstützt .
sigalg	Für den Request wird der Signatur Algorithmus SHA256 mit RSA (**SHA256withRSA)** verwendet. Dies wird für die Requesterzeugung empfohlen. Falls für Ihre Anwendung erforderlich, können Sie auch den Signaturalgorithmus SHA1 verwenden unter Angabe von "**sigalg SHA1withRSA"** während der Requesterzeugung.
dname	Hier folgen die Zertifikats- bzw. Schlüsselangaben. Diese Angaben erscheinen später im Schlüssel und im Zertifikat. Vermeiden Sie die Verwendung von Einträgen, die lediglich ein Leerzeichen enthalten. Soll ein Eintrag, z. B. „Organizational Unit“ nicht verwendet werden, so geben Sie dieses Feld nicht an. Alle unterstützten Zertifikatseinträge werden in der CPS (**C**ertificate **P**ractice **S**tatement) unter Punkt 3 „Identifizierung und Authentifizierung“ aufgelistet:
O	**Organization Name** bzw. Name der Organisation, z. B. **Musterorganisation** Die Verwendung dieses Eintrages ist obligatorisch.
C	**Country Name** bzw. Länderkürzel nach ISO 3166, z. B. **DE** Dieser Eintrag muss in Großbuchstaben erfolgen. Die Verwendung dieses Eintrages ist obligatorisch.
CN	(*, siehe Punkt 2.1.1) **Common Name** bzw. Gemeinsamer Name, z. B. **testhost.example.com** Die Verwendung dieses Eintrages ist obligatorisch.
L	**Locality Name** bzw. Stadt, z. B. **Musterstadt** Die Verwendung dieses Eintrages ist obligatorisch.
OU	**Organizational Unit Name** bzw. Name der Organisationseinheit. Dieses Feld kann bis zu fünfmal vorhanden sein, z. B. **Musterorgansiationseinheit** Die Verwendung dieses Eintrages ist optional.
ST	**State or Province** bzw. Bundesland, z. B. **Bundesland** Die Verwendung dieses Eintrages ist obligatorisch.

PostalCode **Postal Code** bzw. Postleitzahl, z. B. **12345**
Die Verwendung dieses Eintrages ist optional.

STREET **Street Name** bzw. Straßenname, z. B. **Musterstrasse**
Die Verwendung dieses Eintrages ist optional.

Das folgende Kommando erzeugt eine neue Keystore-Datei mit einem neuen Server-Key mit einer Bitlänge von 2048 Bit.

Ist die im Befehl angegebene Keystore-Datei bereits vorhanden, so erzeugt der Befehl in der angegebenen Keystore-Datei einen neuen Eintrag unter dem angegebenen Alias (hier testhost.example.com).
Ist der verwendete Alias bereits vorhanden, so erfolgt eine Fehlermeldung.
Von Java wird standardmäßig das Passwort changeit verwendet. In dieser Anleitung orientieren wir uns an dieser Vorgabe. Wird ein anderes Passwort verwendet, so ist dies in Ihrer Konfiguration oder beim Starten des Webservers zu berücksichtigen. Empfohlen wird, die Passwörter für storepass und keypass gleichnamig zu setzen.

Sollte sich der Java-Pfad nicht in den Umgebungsvariablen des Systems befinden, so führen Sie die im Anschluss aufgeführten Befehle am besten im Java Verzeichnis selbst aus, z. B. „%JAVAHOME%\jre7\bin“

Wichtig: Die hier gezeigten Befehle müssen ohne Zeilenumbruch in der Eingabeaufforderung bzw. Konsole eingegeben werden:

```
keytool -genkey -keyalg RSA -keysize 2048 -alias testhost.example.com -
keystore keystorefile -storepass changeit -keypass changeit -dname "CN=
testhost.example.com, OU=Musterorganisationseinheit, O=Musterorganisation,
L=Musterstadt, ST=Bundesland, C=DE"
```

Die Generierung dauert einige Sekunden. Anschließend liegt das Keystore als Datei vor. Es wird empfohlen, die erzeugte Datei zu sichern, z. B. auf einem externen Medium!

2.1.1 (*) Stichwort „Common Name“ bzw. „Alias“

Für den “Common Name” ist die Adresse des Servers einzutragen, die verschlüsselt werden soll, z.B. testhost.example.com
(In der Regel ist dies der „FQDN“, der **F**ully **Q**ualified **D**omain **N**ame bzw. der eindeutige Name des Internethosts).
Das Feld „Common Name“ bzw. „Alias“ trägt lediglich in dieser Anleitung die Bezeichnung „testhost.example.com“, die Bezeichnung Ihres Servers wird abweichen.
Die Buchstaben des Common Name müssen stets kleingeschrieben werden.
Die Verwendung nichtöffentlicher Einträge, z. B. „localhost“ oder IP-Adressen aus privaten Adressbereichen ist nicht zulässig. Der Eintrag muss gegen öffentliche Registrierungsstellen - wie z. B. „DENIC“ - prüfbar sein.
Bitte beachten Sie hierzu auch die entsprechenden FAQ-Einträge auf unserer Internetseite sowie die zugehörige „CP/CPS TeleSec ServerPass“ (Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb).

2.2 Requesterzeugung

Mit dem soeben erzeugten Schlüssel wird nun ein Request erzeugt:

```
keytool -certreq -alias testhost.example.com -keyalg RSA -sigalg
SHA256withRSA -keystore keystorefile -storepass changeit -keypass changeit -
file requestdatei.pem
```

Durch das Kommando ist die folgende Datei entstanden: **requestdatei.pem**
Es wird empfohlen, die erzeugte Datei zu sichern, z. B. auf einem externen Medium!

Die Server-Zertifikat-Request Datei beinhaltet den Request in dieser Form:

Abbildung 1 (requestdatei.pem)

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBxzCCAtrrtTACAQAwgYYxCzAJBgNVBAYTAkRFMQwwCgYDVQQIEANBgNV
....
DGysW9I7Wv9SOeW5HrhL4SIlzVVVzFUW5NvRpQCaE+qIkpo+w9l5K0/HFn5mWSkT
cPMXx5uYkJNO8l9REmvcJMhvJIzw4vP+kyjM
-----END CERTIFICATE REQUEST-----
```

2.3 Beauftragung des Serverzertifikats

Nachdem der Request erzeugt wurde, können Sie auf unserer Internetseite einen ServerPass bzw. einen ServerPassTest beauftragen.

https://www.telesec.de/serverpass/ (→ myServerPass Kundenportal)

Auf der Webseite können Sie sich mit Benutzername und Kennwort anmelden bzw. falls erforderlich, sich zunächst für myServerPass registrieren.

Nach erfolgreicher Anmeldung wählen Sie den Menüpunkt „Zertifikat beauftragen“ und anschließend „Beauftragen Sie hier“.

Möchten Sie ein SAN-Zertifikat oder ein Zertifikat mit „Extended Validation“ beauftragen, so beachten Sie bitte die entsprechenden Hinweise der bereitgestellten Zusatzinformationen auf unserer Internetseite.

Zunächst wählen Sie die gewünschte Root aus, i. d. R. ist dies „TeleSec-CA-2“ aus. Anschließend wird das gewünschte Produkt bzw. die gewünschte Laufzeit des beauftragten Zertifikats festgelegt.

In das Feld " **Mein PKCS#10 Zertifikats-Request**" kopieren Sie den Request aus Abbildung 2 oben, inklusive der „----BEGIN.... und ----END... “ Zeilen per cut & paste.

Abbildung 2

Nach dem Einfügen werden die Request-Inhalte zur Kontrolle angezeigt,
siehe rote Markierung in Abbildung 2 unten.

Füllen Sie alle weiteren Felder entsprechen Ihrer Vorgaben aus und senden den Online-Auftrag ab.
Das Auftragsformular für den Serverpass wird nach dem Absenden zum Abspeichern bzw. Ausdrucken angeboten. Alternativ können Sie sich das Formular per Email zuschicken lassen. Hierbei wird das Auftragsformular als PDF-Datei zur Verfügung gestellt.
Bitte notieren Sie sich die Referenznummer des Auftrages.

Senden Sie das geprüfte und unterschriebene Auftragsformular mit den benötigten Authentifikations-Unterlagen an die aufgedruckte Anschrift.
Der technische Ansprechpartner erhält erst nach erfolgreicher Prüfung eine Email-Benachrichtigung über die Ausstellung des Zertifikats.

2.4 Herunterladen und Import der Zertifikate

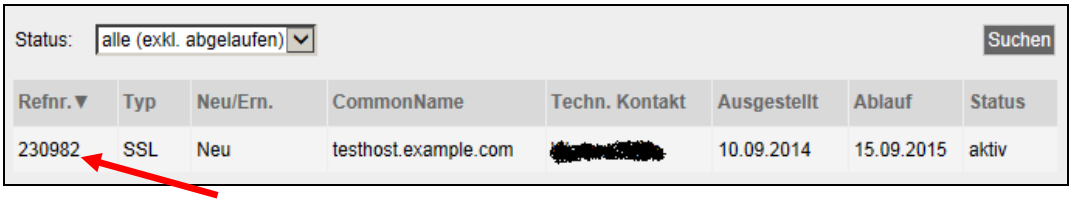
2.4.1 Herunterladen der Zertifikate

Anmelden im Webportal „myServerPass“:
www.telesec.de/serverpass/index.html (→ myServerPass)

Wählen Sie den Menüpunkt „Meine Zertifikate“

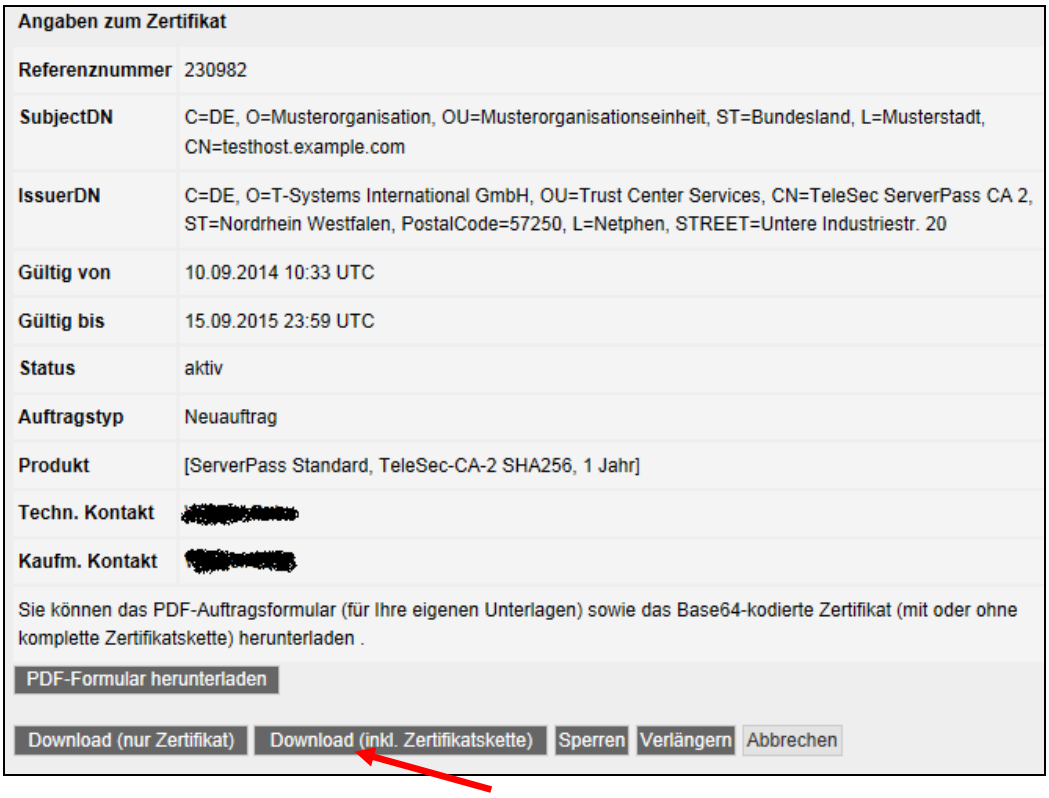
Hier werden nun alle Ihre Zertifikate aufgelistet.
Wählen Sie das herunter zuladende Zertifikat durch Klick auf die Referenznummer aus, siehe Abbildung 3.

Abbildung 3:



Es werden zwei Download-Formate angeboten, siehe auch Abbildung 5:
- Download (Nur Zertifikat)
- Download (inkl. Zertifikatskette)

Abbildung 4



Wählen Sie das Format: „Download inkl. Zertifikatskette“.
Aktivieren Sie die Option „Als Datei speichern und legen einen Dateipfad fest, z. B. c:\

Sie erhalten die Datei „servpass-123456-x509chain.pem“ und sie liegt nun in diesem Verzeichnis: c:\ servpass-123456-x509chain.pem

2.4.2 Import der Zertifikate

So wie in Abbildung 5 dargestellt, enthält die herunter geladene Datei mehrere Zertifikate. Im Einzelnen sind dies:

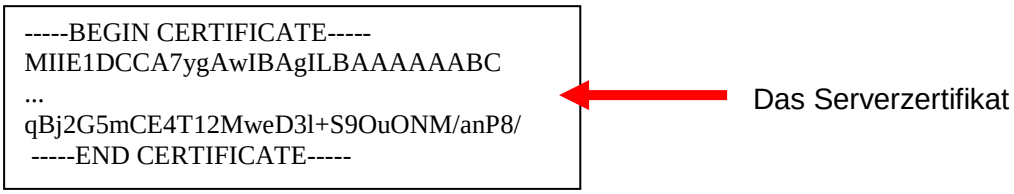
1. Das eigentliche „Serverzertifikat“, auch User-Zertifikat genannt.
2. Das Zertifikat „TeleSec ServerPass CA 2“, auch CA-Zertifikat genannt.
3. Das Zertifikat „Baltimore CyberTrust Root“ Zertifikat, auch Root-Zertifikat genannt.

Abbildung 5 (servpass-123456-x509chain.pem)

```
# Ihr ServerPass Zertifikat:
# -------------------------
#   Subject:
C=DE,O=Musterorganisation,OU=Musterorganisationseinheit,ST=Bundesl
and,L=Musterstadt,CN=testhost.example.com
#   Issuer: C=DE,O=T-Systems International GmbH,OU=Trust Center
Services,CN=TeleSec ServerPass CA 2,ST=Nordrhein
Westfalen,PostalCode=57250,L=Netphen,STREET=Untere Industriestr.
20
#   Ser.No.: 0x7d5da7c89d79451f
-----BEGIN CERTIFICATE-----
MIIFxjCCBK6gAwIBAgICQBMwDQYJKoZIhvcNAQEFBQAwgYIxCzAJBgNVBAYTAkRF
...
OGAb1gNE4cu5uYPKtTLbFVyaZ6EhHUoM00Vwl63lU9TUhClrEUZUb5HJ
-----END CERTIFICATE-----
#
# CA Zertifikat:
#-------------------------
#   Subject: C=DE,O=T-Systems International GmbH,OU=Trust Center
Services,CN=TeleSec ServerPass CA 2,ST=Nordrhein
Westfalen,PostalCode=57250,L=Netphen,STREET=Untere Industriestr.
20
#   Issuer: C=IE,O=Baltimore,OU=CyberTrust,CN=Baltimore CyberTrust
Root
#   Ser.No.: 0x727b216
 -----BEGIN CERTIFICATE-----
lkjlhGUkjhkljLKLKKJJLKhguGugtuigjkZIU.
...
9OuONM/anP8/AdEIZ6ziGwdUpRzLlO8eA==
-----END CERTIFICATE-----
#
# Root Zertifikat:
# ----------------
#   Subject: C=IE,O=Baltimore,OU=CyberTrust,CN=Baltimore CyberTrust Root
#   Issuer: C=IE,O=Baltimore,OU=CyberTrust,CN=Baltimore CyberTrust Root
#   Ser.No.: 0x020000b9
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILAgAAzELMAkG
...
Zg6C3ZjL2sJETy6ge/L3ayx2EYRGinij4w==
-----END CERTIFICATE-----
```

Öffnen Sie die herunter geladene Datei mit einem einfachen Texteditor z. B. Wordpad, ggf. muss bei Öffnen der Dateityp „Alle Dokument *.*“ eingestellt werden.
Markieren Sie das Server bzw. User-Zertifikat incl. der ---BEGIN... und ---END... Zeilen (hier blau unterlegt) und speichern es als Textdokument in einer eigene Datei ab, z. B. „usercert.crt“, siehe Abbildung 6.

Abbildung 6: (usercert.crt)



Nach dem gleichen Schema werden nun die CA- und das Root-Zertifikat behandelt:

CA-Zertifikat: Markieren Sie das CA-Zertifikat „TeleSec ServerPass CA 2“ incl. der ---BEGIN... und ---END... Zeilen (hier magenta markiert) und speichern es als Textdokument in eine eigene Datei ab, z. B. „ServerPass-CA2.crt“.
Sollten in der herunter geladenen Datei mehrere CA-Zertifikate aufgelistet werden, so verfahren Sie mit diesen CA-Zertifikaten analog.

Root-Zertifikat: Markieren Sie das Root-Zertifikat Baltimore Cybertrust Root CA incl. der ---BEGIN... und ---END... Zeilen (hier grün markiert) und speichern es als Textdokument in eine eigene Datei ab, z. B. „BaltimoreCyberTrustRoot.crt“

Zuerst muss stets das Root Zertifikat in die Keystore-Datei importiert werden. Achten Sie immer auf den Import des korrekten Zertifikats!
Beinhaltet die Keystore-Datei bereits das Root Zertifikat, so erübrigt sich ein erneuter Import.
Folgendes Kommando importiert das Root-Zertifikat unter dem Alias „BaltimoreCyberTrustRoot“:

```
keytool -import -file BaltimoreCyberTrustRoot.crt -alias rootcert -keystore
keystorefile   -storepass changeit -keypass changeit
```

Die aufkommende Frage „Diesem Zertifikat vertrauen?“ bzw. „Trust this certificate?“ bestätigen Sie mit ja bzw. yes.
Er erfolgt die Meldung: „Zertifikat wurde zum Keystore hinzugefügt“ bzw. „Certificate was added to keystore“

Nach dem gleichen Schema wird nun das CA-Zertifikat importiert.
Beinhaltet die Keystore-Datei bereits das CA Zertifikat, so erübrigt sich ein erneuter Import

Folgendes Kommando importiert das CA Zertifikat unter dem Alias „ServerPass-CA2 “:

```
keytool -import -file ServerPass-CA2.crt -alias ServerPass-CA2 -keystore
keystorefile -storepass changeit -keypass changeit
```

Als letztes wird das Serverzertifikat importiert.
Wichtig ist hierbei, dass der verwendete Alias mit dem Alias des in Schritt 1 erzeugten Schlüssels übereinstimmt, z. B. „testhost.example.com“.
Auch beim Import eines verlängerten Zertifikats muss der verwendete Alias dem Eintrag der ursprünglichen Keystore- bzw. Requesterzeugung entsprechen.
Folgendes Kommando importiert das Serverzertifikat Zertifikat unter dem Alias „testhost.example.com“:

```
keytool -v -import -file usercert.crt -alias testhost.example.com -keystore keystorefile
-storepass changeit  -keypass changeit
```

Er erfolgt die Meldung: „Zertifikatsantwort wurde in Keystore installiert“ bzw. „Certificate reply was installed in keystore“.

Der Import der Zertifikate ist nun abgeschlossen.

Somit verfügt man über eine vollständige Keystore-Datei für die weitere Verwendung in einem Java basierendem Webserver, der einen Java Keystore benötigt.

Durch das folgende Kommando kann man sich alle in der Keystore-Datei enthaltenen Einträge auflisten lassen:

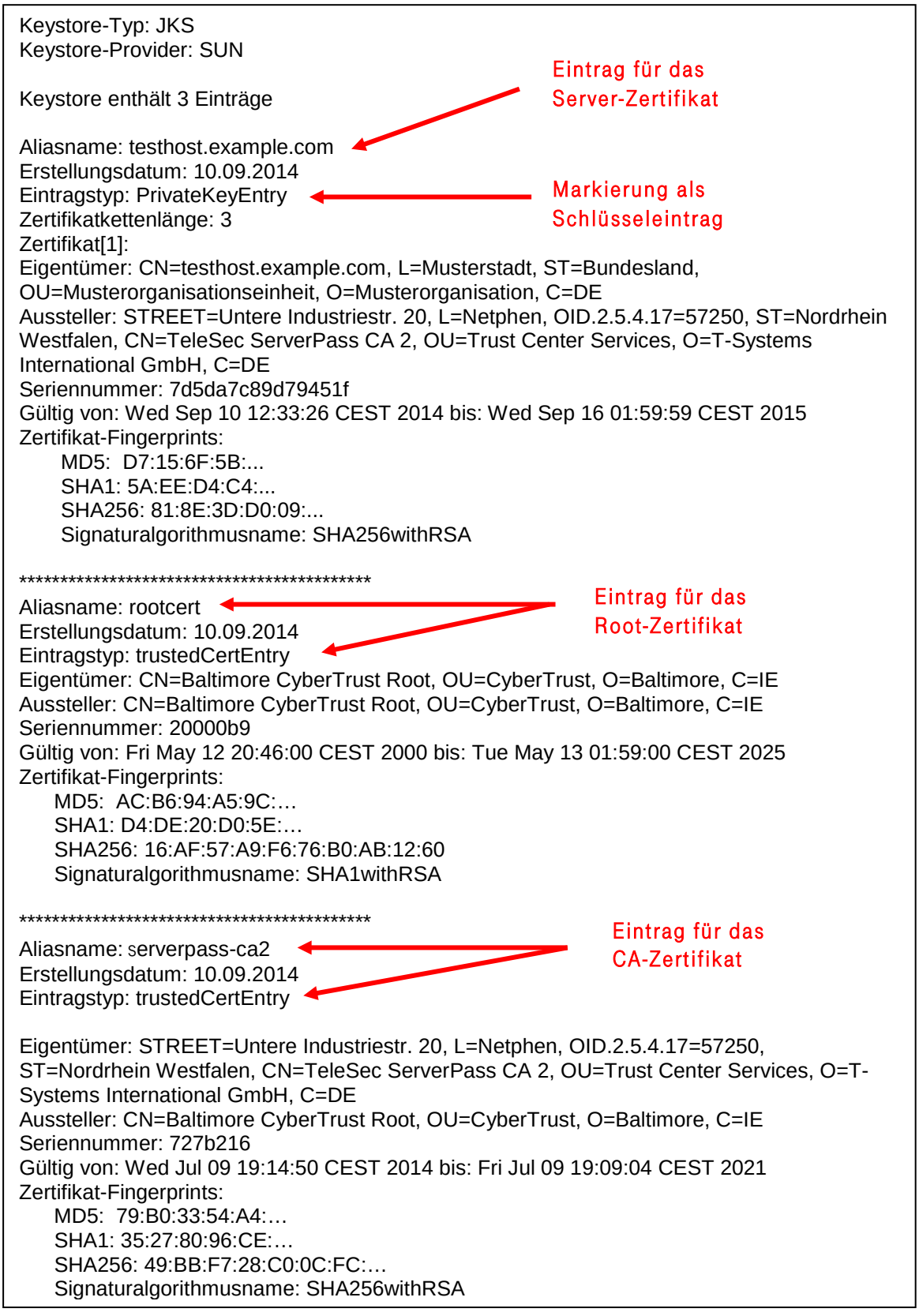
```
keytool -list -v -keystore keystorefile -storepass changeit  -keypass changeit
```

Abbildung 8 stellt die Inhalte des Keystores exemplarisch dar.

Wichtig:
unter dem Aliasnamen Ihres Serverzertifikats muss dieser Eintrag erscheinen:
"**Eintragstyp: PrivateKeyEntry**"

Ansonsten können Sie das keystore nicht bestimmungsgemäß verwenden.

Abbildung 7 (Anzeige der Keystore-Inhalte)



2.5 Sicherung der Dateien

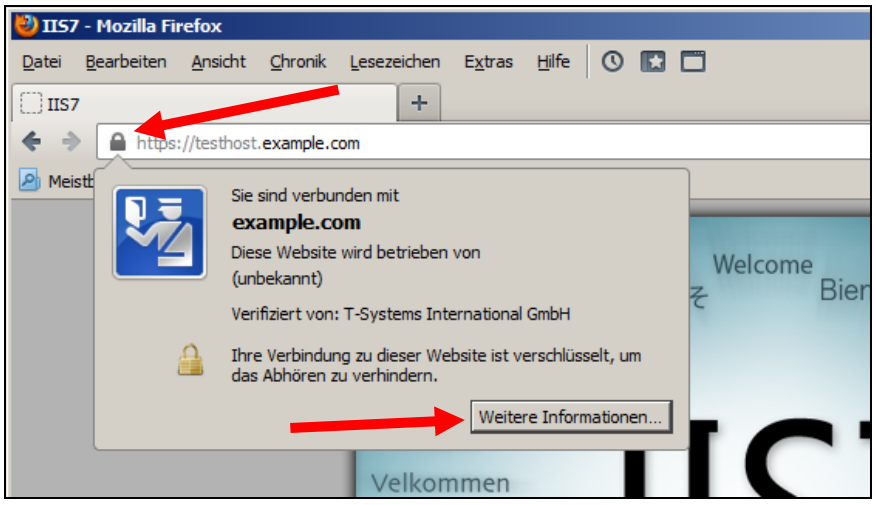
Es wird dringend empfohlen, die erzeugten Dateien zu sichern, z. B. auf einem externen Medium!

3 Kontrolle

Für die Kontrolle empfiehlt sich der Aufruf der abgesicherten Webseite über einen externen Browserclient, also nicht vom Server selbst. Beim Aufruf der abgesicherten Seite,
z. B. „https://testhost.example.com“ wird der SSL-Modus durch ein Schloss neben der Adressleiste symbolisiert. Andere Browser stellen den SSL-Modus ggf. anders dar. Exemplarisch ist hier die Darstellung im Firefox (Abbildung 8 -10) sowie im Internet Explorer (Abbildung 11- 12) aufgeführt.

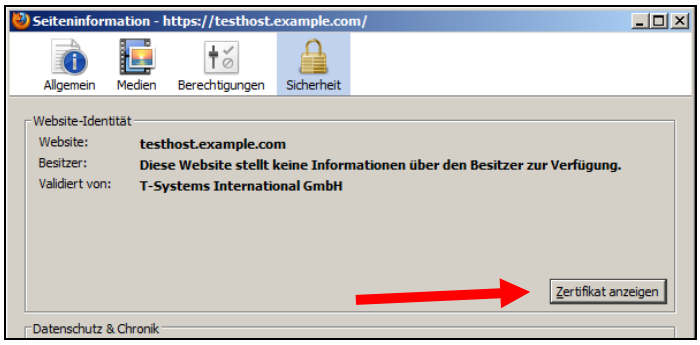
Firefox:

Abbildung 8 (Firefox 21):



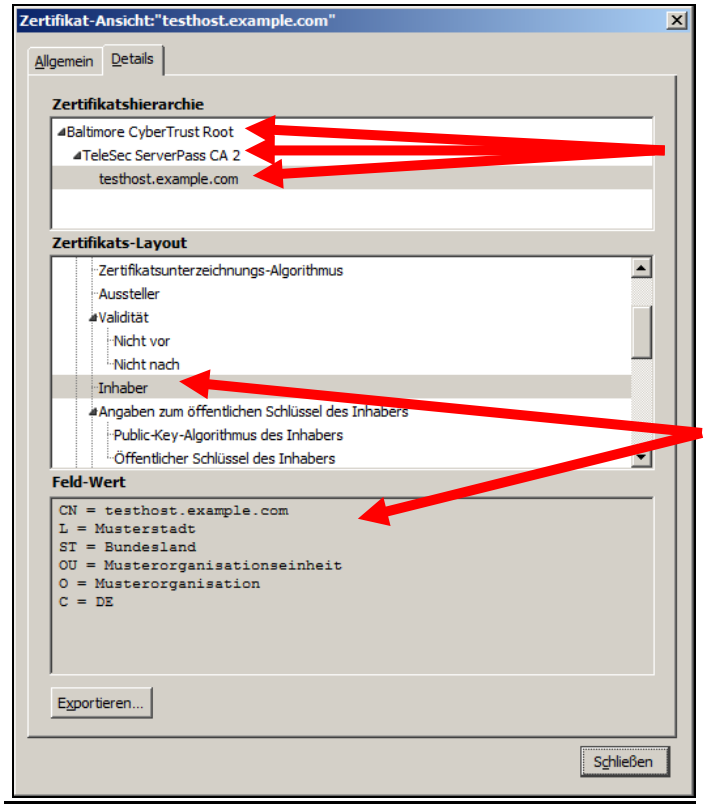
Beim Firefox lassen sich über einen Klick auf das Schloss Details zum verwendeten Zertifikat anzeigen.
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 9 (Firefox 21):



Wählen Sie „Zertifikat anzeigen“.

Abbildung 10 (Firefox 21):



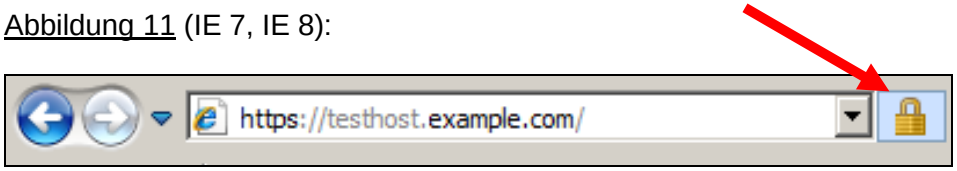
Darstellung der kompletten Zertifikatskette

Zertifikatdetails

Durch Auswahl des Reiters „Details“ lässt sich die Zertifikatshierarchie anzeigen.
Um einzelne Zertifikatseinträge darzustellen, markieren Sie zunächst ein Zertifikat und dann den gewünschten Eintrag unter „Zertifikats-Layout“

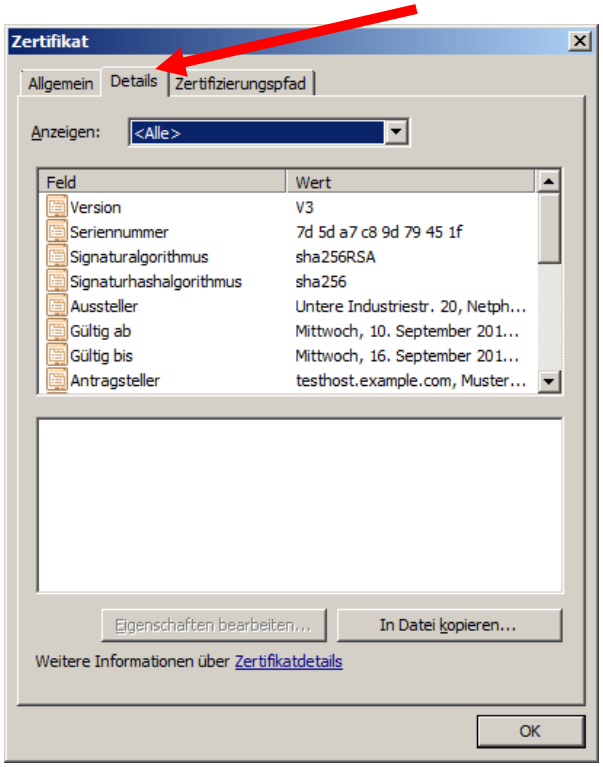
Internet Explorer

Abbildung 11 (IE 7, IE 8):



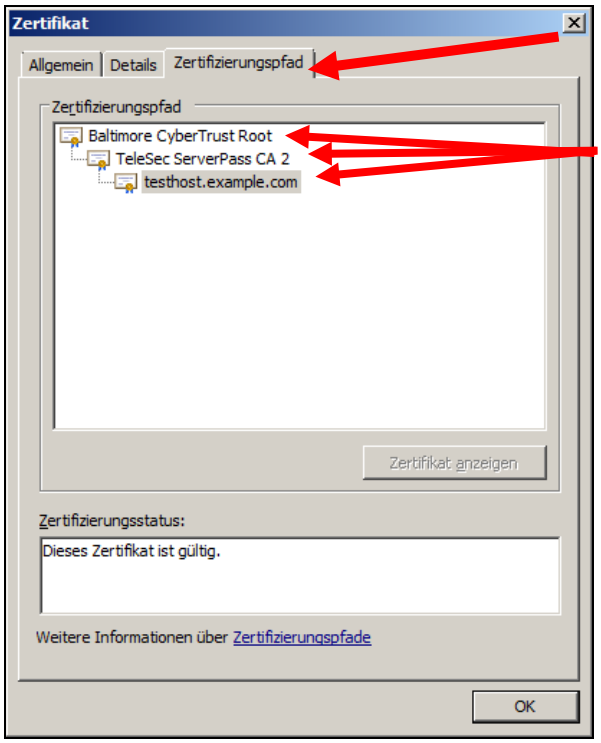
Beim Internet Explorer lassen sich die Zertifikatsdetails durch Doppelklick auf das Schloss anzeigen.
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 12.

Abbildung 12 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 13.

Abbildung 13 (Die Zertifikatskette)



Darstellung der kompletten Zertifikatskette

So wie in Abbildung 13 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.

4 Zertifikat erneuern

Das durch die Erneuerung erzeugte Zertifikat wird alle Einträge (Common Name, Organisation usw.) des zu erneuernden Zertifikats tragen. Gültigkeit, Fingerprints, Referenz- und Seriennummer werden neu gesetzt.

Unabhängig von der Restlaufzeit des zu erneuernden Zertifikats wird das neue Zertifikat sofort ausgestellt und steht zum Download bereit.

Durch die Erneuerung wird das zu erneuernde Zertifikat nicht gesperrt, es bleibt bis zum Ende seiner Laufzeit bzw. bis zu einer eventuellen Sperrung gültig.

4.1 Bedingungen für eine Zertifikatserneuerung

Die Erneuerungsoption im Kundenportal kann nicht genutzt werden sofern:

- das zu erneuernde Zertifikat gesperrt wurde
- das zu erneuernde Zertifikat bereits abgelaufen ist
- das neue Zertifikat andere Zertifikatsinhalte tragen soll als das zu Erneuernde
- das zu erneuernde Zertifikat wird nicht in der Liste unter „Meine Zertifikate“ aufgeführt
- das verwendete Schlüsselmaterial des zu erneuernden Zertifikats wird nicht länger als sicher eingestuft. z. B. aufgrund der Schlüssellänge oder des verwendeten Algorithmus. So gelten Schlüssel mit eine Schlüssellänge kleiner 2048 Bit nicht länger als sicher und werden sind von der Beauftragung ausgeschlossen.
- Das zu erneuernde Zertifikat enthält Einträge oder Eigenschaften, die nicht länger unterstützt werden

Kann die Erneuerungsfunktion aus irgendeinem Grunde nicht verwendet werden, so nutzen Sie bitte die Option „Zertifikat beauftragen“ im Kundenportal myServerPass.

Achtung: eine nochmalige Verwendung eines bereits für ein Zertifikat verwendeten Server-Schlüssels ist nicht zulässig und wird vom System abgewiesen.
Daher ist ggf. die Erzeugung eines neuen Server-Schlüssels sowie eines neuen Zertifikat-Requests erforderlich. Folgen Sie hierzu bitte der Anleitung:
Anschließend wird die Requesterzeugung erneut angestoßen.

Folgen Sie dieser Anleitung von Beginn an unter Berücksichtigung der in Punkt 4.2 angegebenen Hinweise.

4.2 Besonderer Hinweis für eine Zertifikats-Erneuerung mit Java Keytool

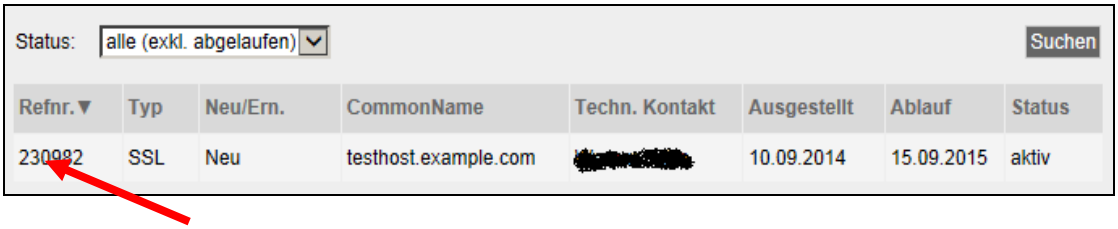
In der Regel ist die Erzeugung eines weiteren Requests nicht erforderlich.

Steht der private Schlüssel des zu verlängernden Zertifikats nicht mehr zur Verfügung, muss zunächst ein neuer Keystore mit neuem Schlüssel und anschließend ein neuer Request erzeugt werden.

Hierbei müssen die gleichen Angaben (Organisation, Organisationseinheit, Common Name, Stadt, Bundesland, Staat, evtl. auch Strasse und Postleitzahl) gemacht werden, wie bei der Beauftragung des zu erneuernden TeleSec ServerPass Zertifikats. Die Angaben des zu erneuernden Zertifikates lassen sich z. B. im Servermanager anschauen.

Melden Sie sich am Kundenportal „myServerPass“ an.
Unter dem Menüpunkt “Meine Zertifikate“ erscheint eine Liste aller Ihrer Zertifikate, siehe Abbildung 14.

Abbildung 14: (Ausschnitt des Kundenportals):



Hier können Sie nun das zu erneuernde Zertifikat anhand der Referenznummer ermitteln. Lassen Sie sich die Zertifikatseinträge durch Klicken auf die „Referenznummer“ oder den „Common Name“ anzeigen, siehe Abbildung 15.

Abbildung 15: (Zertifikatsdetails)

Die relevanten Daten befinden sich im Abschnitt „SubjectDN“.
Anhand der ermittelten Daten kann gemäß Punkt 2.1 und 2.2 ein neues Keystore mit neuem Schlüssel sowie ein neuer Request erzeugt werden.

4.3 Erneuerung durchführen

Melden Sie sich am Kundenportal „myServerPass“ an.
Unter dem Menüpunkt “Meine Zertifikate“ erscheint eine Liste aller Ihrer Zertifikate, siehe Abbildung 15.
Hier können Sie nun das zu erneuernde Zertifikat anhand der Referenznummer ermitteln. ggf. lassen sich die Zertifikatseinträge durch Klicken auf die „Referenznummer“ oder den „Common Name“ anzeigen, siehe Abbildung 15.

Abbildung 16: (Ausschnitt des Kundenportals):

Nachdem das zu erneuernde Zertifikat ermittelt wurde, klicken Sie den Button „Verlängern“. Anschließend bekommt man die Zertifikatsdaten des zu erneuernden Zertifikats angezeigt.

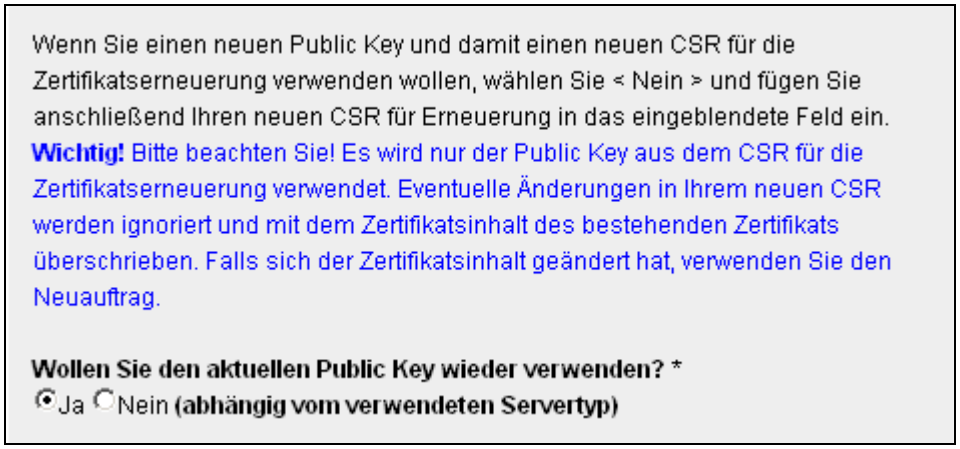
Treffen Sie die gewünschte Root- sowie Produkt-Auswahl (Laufzeit).

Anschließend wird die Verwendung des Public Keys abgefragt, siehe Abbildung 17.

4.4 Die Verwendung des Public Keys bei der Erneuerung

Bei einer Erneuerung stehen zwei Optionen zur Auswahl, siehe Abbildung 17:

Abbildung 17: (Verwendung des Public Keys)



4.4.1 Erneuerung unter Wiederverwendung des Public Keys

Sofern der private Schlüssel des zu verlängernden Zertifikats vorhanden ist, muss nicht zwingend ein neuer Request erzeugt werden, man kann hier die Option „Ja“ auswählen und den Onlineauftrag absenden.
Er wird ein Zertifikat unter Verwendung des öffentlichen Schlüssels des zu erneuernden Zertifikats erzeugt.

4.4.2 Erneuerung unter Verwendung eines neuen Public Keys

Wurde ein Request unter Verwendung eines neuen privaten Schlüssels erzeugt,
so wählen Sie bei der Frage „Wollen Sie den aktuellen Public Key wieder verwenden?“ die Option „Nein“ und kopieren den neu erzeugten Request in das Feld " **Mein PKCS#10 Zertifikats-Request**" (inklusive der ----BEGIN.... und ----END... Zeilen).
Nach dem Einfügen werden die Request-Inhalte zur Kontrolle angezeigt,
siehe Abbildung 18.

Abbildung 18:

Prüfen Sie die angezeigten Zertifikatsdaten sowie Ihre Kontaktdaten und senden das Formular ab.

Es wird ein Zertifikat unter Verwendung der Schlüsselkennung des Public Keys des soeben eingestellten Request erzeugt.
Zu Grunde gelegt werden die Zertifikatsinhalte (Common Name, Organisation usw.) des zu erneuernden Zertifikats. Eventuell anders lautende Angaben des Requests werden überschrieben.

4.5 Verwendung des erneuerten Zertifikats

Das Herunterladen sowie der Import der Zertifikate geschieht gemäß Punkt 2.4 ff dieser Anleitung.