TeleSec ServerPass

Zertifikat-Requesterzeugung mit dem Oracle iPlanet 7 Webserver

Version: 1.1
Stand: 14.04.2014
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_oracle_iplanet_7_webserver.doc		Requesterzeugung Oracle iPlanet 7 Webserver

Version	Stand	Status
1.1	19.02.2013	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
Zertifikat-Requesterzeugung mit dem Oracle iPlanet 7 Webserver

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	16.02.2013	Trust Center T-Systems, ASC	Erster Entwurf
1.0	19.02.2013	Trust Center T-Systems, ASC	Inhalt- und Layoutanpassung
1.1	10.04.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

1 Allgemeines

Dieses Dokument beschreibt die Requesterzeugung sowie die Einbindung der Zertifikate im Oracle iPlanet 7 Webserver.

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.

Diese Anleitung beschreibt lediglich die Erzeugung eines Server-Zertifikat-Request sowie die Einbindung der Zertifikate im Webserver. Der Webserver ist somit in der Lage, verschlüsselte Verbindungen über https aufzunehmen.
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 Office-Paketen 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 bezl. des erlaubten Zeichensatzes ab Kapitel 8.3.

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 von Server-Zertifikaten mehrere CA-Zertifikate zum Einsatz kommen, 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 einmal für eine Beauftragung verwendet werden.
Werden mehrere Zertifikate benötigt, so müssen jeweils separate Schlüssel und Requests 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 Oracle iPlanet 7 Webserver

Die Beschreibung bezieht sich auf folgende Softwarekonstellation:

Plattform: Microsoft Server 2008 R2
Oracle iPlanet 7.0 Webserver
Beliebiger Internetbrowser, hier Firefox 18

Voraussetzung: Der Webserver startet bereits im unverschlüsselten Modus

Im Beispiel wird die Administration über die webbasierte „Administration Console“ beschrieben.

1.2.1 Vorbereiten des Webservers

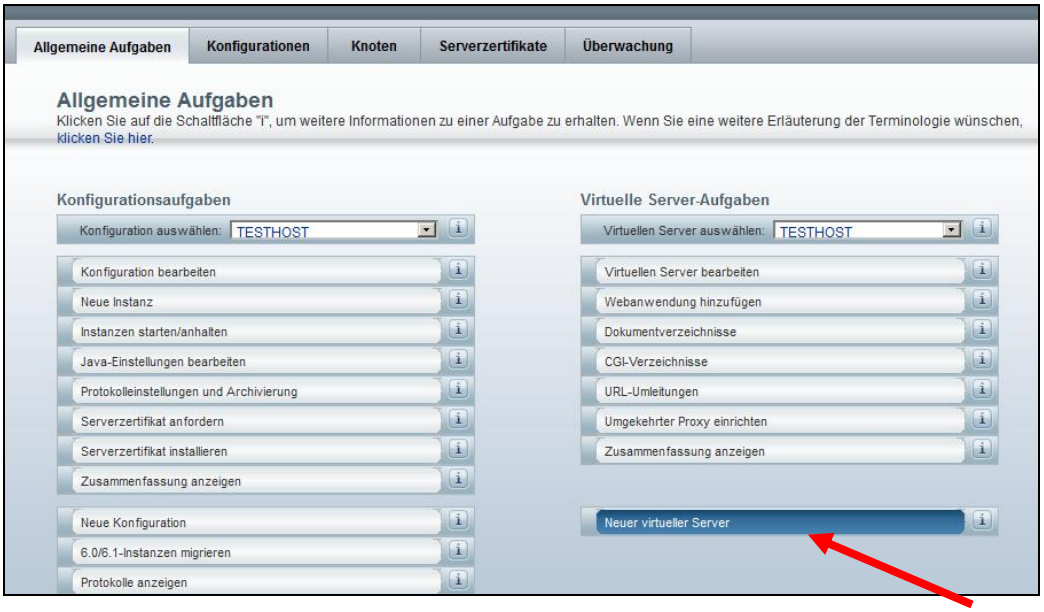
Diese Kurzanleitung dient lediglich als Installationshilfe. Es wird nicht auf die einzelnen Einstellungsmöglichkeiten des Oracle iPlanet 7 Webservers eingegangen. Weiterführende Informationen erhalten Sie in der Dokumentation des iPlanet Webservers.
Gezeigt wird hier lediglich eine Minimalkonfiguration, um den Webserver im SSL-Modus betreiben zu können
Wir gehen hier von einer Standardinstallation und einem Standardbetrieb des Webservers aus.
Das bedeutet: es wurde bereits ein betriebsfähiger Oracle iPlanet 7 Webserver installiert und nun soll zusätzlich zur Standardverbindung auch eine verschlüsselte Verbindung per SSL zum Server ermöglicht werden.

Sollten Sie die Vorbereitungen schon durchgeführt haben, so können Sie diesen Schritt überspringen.

Standardmäßig antwortet der Webserver auf Anfragen per http auf Port 80.
Um zusätzlich auch verschlüsselte Anfragen zu ermöglichen, wird im Beispiel ein weiterer Virtueller Server eingerichtet, der Anfragen per https auf Port 443 entgegennimmt.
Andere Vorgehensweisen sind ebenfalls möglich

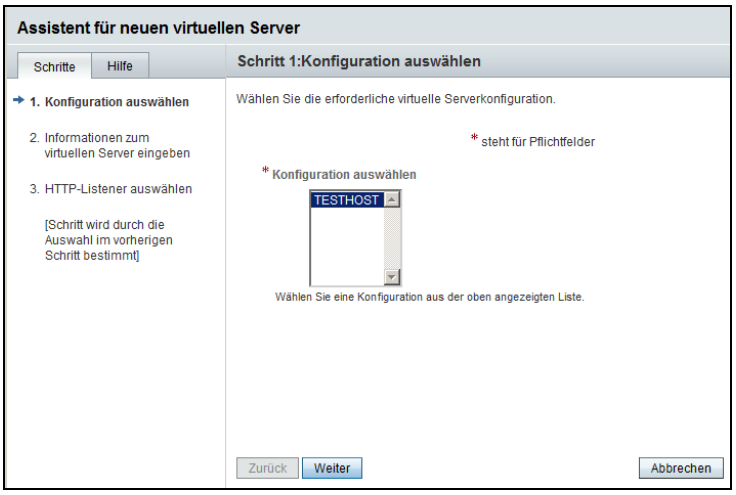
Die Konfiguration geschieht über die Administration des iPlanet, siehe Abbildung 1

Abbildung 1



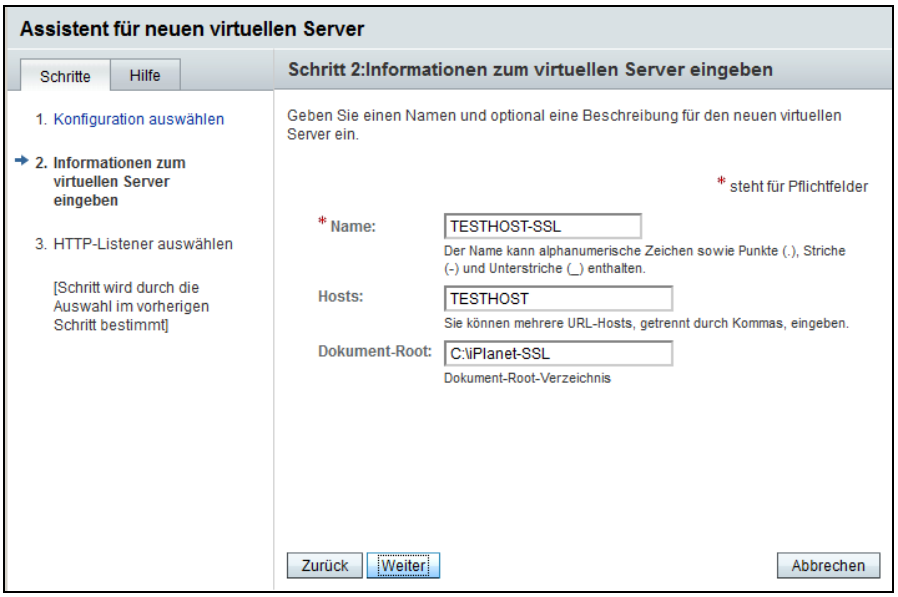
Nach der Anmeldung an der „Administration Console“ stehen alle Konfigurationsaufgaben zur Auswahl bereit.
Wählen Sie den Reiter „**Allgemeine Aufgaben**“ und unter dem Menü „**Virtuelle Server-Aufgaben**“ den Punkt „**Neuer virtueller Server**“.

Abbildung 2



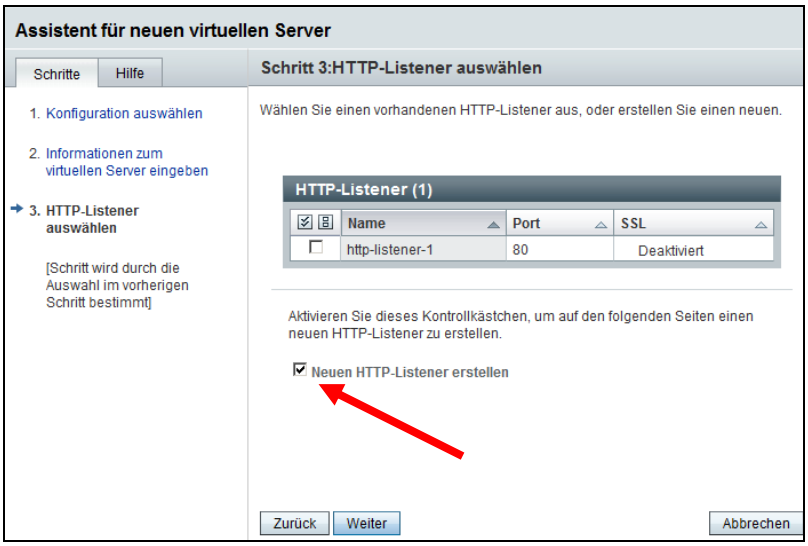
Wählen Sie die gewünschte Konfiguration aus und klicken auf „**Weiter**“.

Abbildung 3



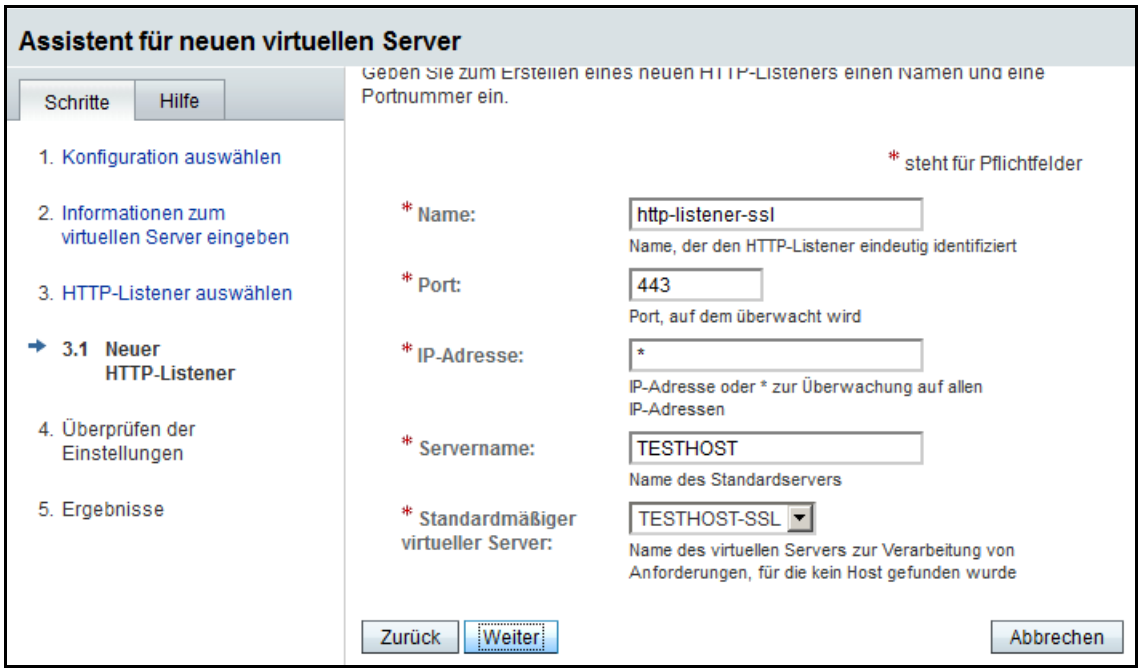
Vergeben Sie einen Namen für den neuen virtuellen Server sowie den Pfad zu den Webdokumenten (Dokument-Root).

Abbildung 4



In der nächsten Abbildung wird die Erstellung eines neuen http-Listeners angestoßen. Hierin wird u. a. der Port für die SSL-Verbindungen festgelegt, siehe Abbildung 5.

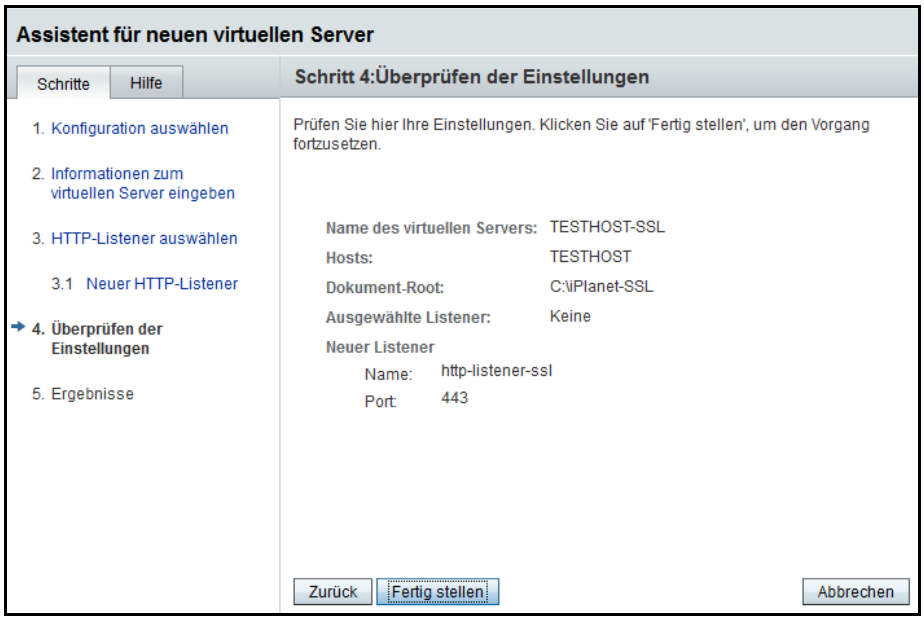
Abbildung 5



Für den neuen HTTP-Listener können die Angaben gemäß Abbildung 5 festgelegt werden. Standardmäßig wird dieser Port verwendet: **443**.

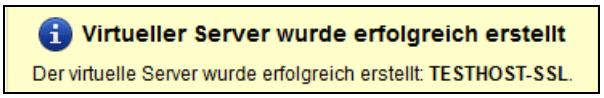
Falls der Bereich für SSL erscheinen sollte, der „SSL-Modus“ wird hier noch nicht aktiviert.

Abbildung 6



Gemäß Abbildung 6 lassen sich die Einstellungen überprüfen und „**Fertig stellen**“.

Abbildung 7



Der neue virtuelle Server wurde erfolgreich angelegt.

Abbildung 8

In der Konfiguration wird nun der neue virtuelle Server aufgelistet.
Die Änderungen müssen über den Link „**Bereitstellung steht aus**“ aktiviert werden.

Abbildung 9

Über „**Bereitstellen…**“ werden die Änderungen übernommen.

Abbildung 10

Damit die Änderungen wirksam werden, müssen die Instanzen neu gestartet werden.

Abbildung 11

Der erfolgreiche Neustart wird entsprechend quittiert.

Die Vorbereitung ist hiermit abgeschlossen und die Requesterzeugung kann beginnen.

2 Requesterzeugung, Beauftragung, Installation, Sicherung des privaten Schlüssels

2.1 Requesterzeugung

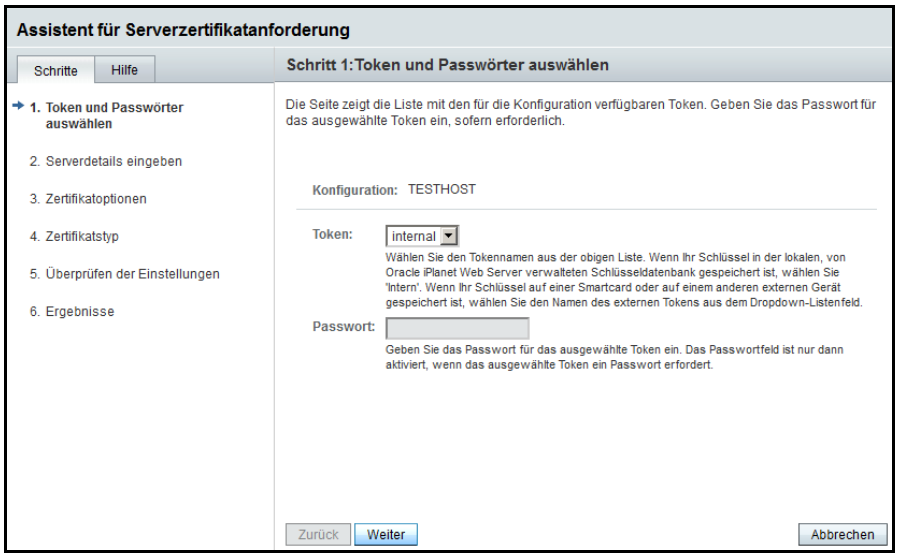
In dieser Anleitung wird kein Passwort zum Schutz der Zertifikate vergeben. Wenn gewünscht, kann über den Reiter „PKCS11-Token“ ein Passwort definiert werden. Wurde ein Passwort definiert, so muss es bei den nachfolgenden Aktionen immer wieder eingegeben werden.

Abbildung 12

Nun wird die Requesterzeugung angestoßen.

Dies geschieht im Reiter „Serverzertifikate“ über „**Anforderung…**“

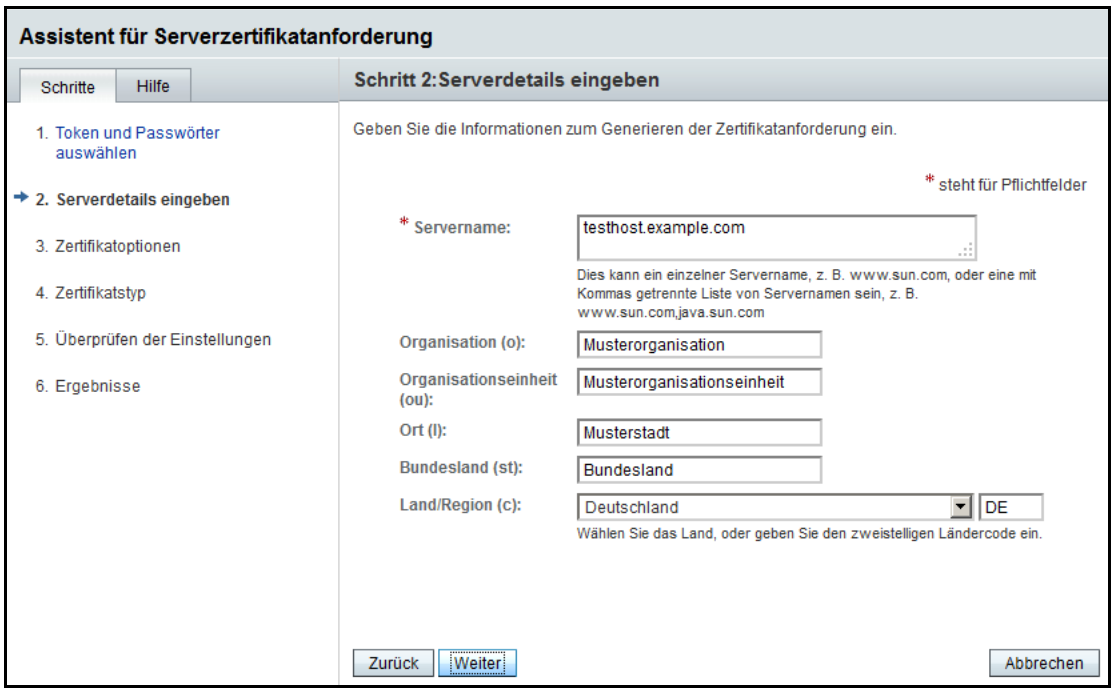
Abbildung 14



Es öffnet sich der Assistent für die Serverzertifikatinstallation.

Wählen Sie unter Token „**Internal**“ aus und tragen ggf. Ihr zuvor definiertes Passwort ein.

Abbildung 15



Nun werden die einzelnen Zertifikatseinträge festgelegt, diese Angaben erscheinen später unverändert im Zertifikat, im Einzelnen sind dies die folgenden Einträge.

Beschreibung der Zertifikatseinträge:

„Gemeinsamer Name“ Hier „Servername“	(*, siehe Punkt 2.1.1) Common Name bzw. Gemeinsamer Name, z. B. **testhost.example.com** Die Verwendung dieses Eintrages ist obligatorisch.
„Organisation“	Organization Name bzw. Name der Organisation, z. B. **Musterorganisation** Die Verwendung dieses Eintrages ist obligatorisch.
„Organisationseinheit“	Organizational Unit Name bzw. Name der Organisations-einheit, z. B. **Musterorgansiationseinheit** Die Verwendung dieses Eintrages ist optional.
„Ort“	Locality Name bzw. Stadt, z. B. **Musterstadt** Die Verwendung dieses Eintrages ist obligatorisch.
„Bundesland/ Kanton”	State or Province bzw. Bundesland, z. B. **Bundesland** Die Verwendung dieses Eintrages ist obligatorisch.
„Land/ Region“	Name bzw. Länderkürzel nach ISO 3166, z. B. **DE** Die Verwendung dieses Eintrages ist obligatorisch.

Bitte beachten Sie für die Requesterzeugung die in unseren CPS (**C**ertificate **P**ractice **S**tatement) aufgeführten Hinweise. Insbesondere den erlaubten Zeichensatz.
Siehe hierzu: www.t-systems-telesec.com (→ Online Auftrag → Telekom Zertifikate)

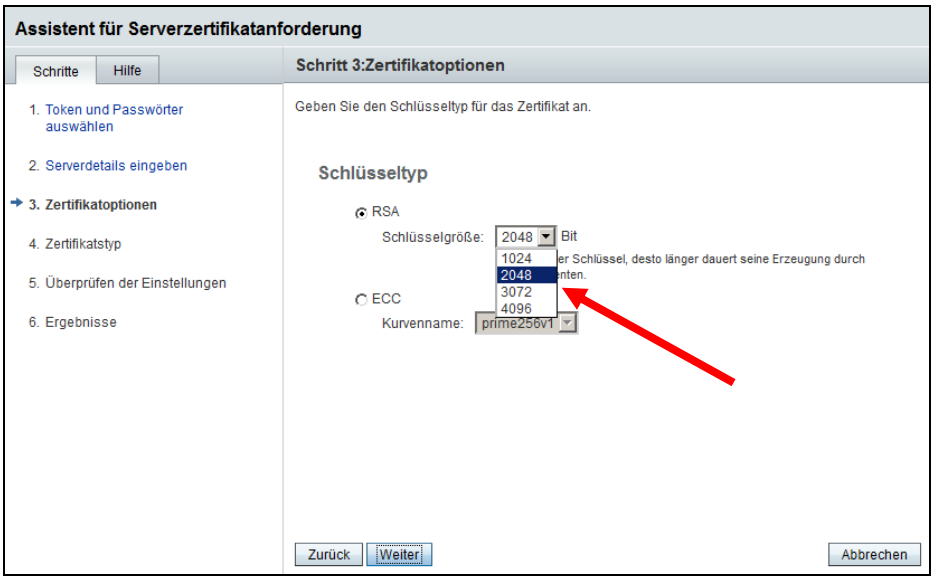
Vermeiden Sie die Verwendung von Feldern, die lediglich ein Leerzeichen enthalten!

2.1.1(*) Stichwort „Common Name“

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 sind 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 „CPS“ (**C**ertificate **P**ractice **S**tatement).

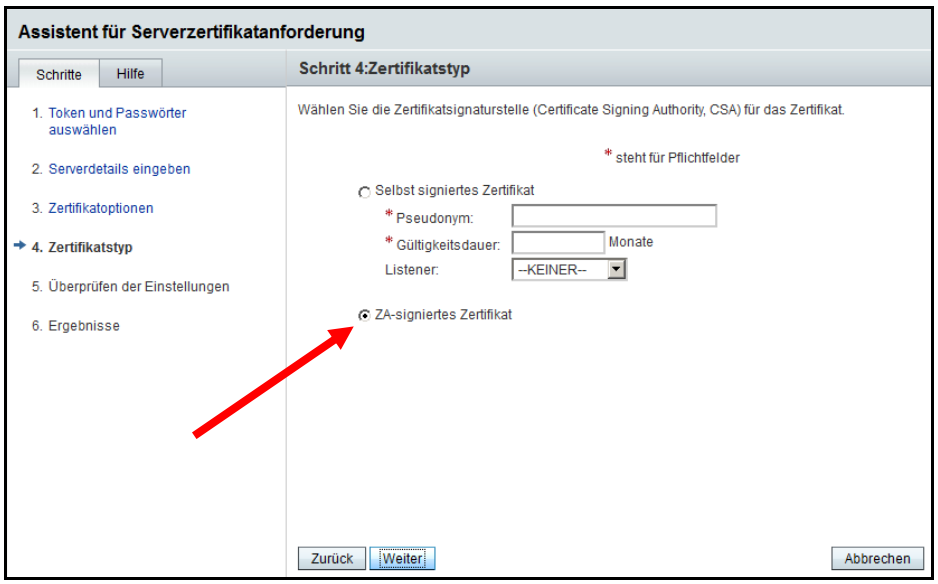
Nachdem alle Angaben gemacht wurden, gelangen Sie über den Button „**Weiter**“ zu Abbildung 16.

Abbildung 16



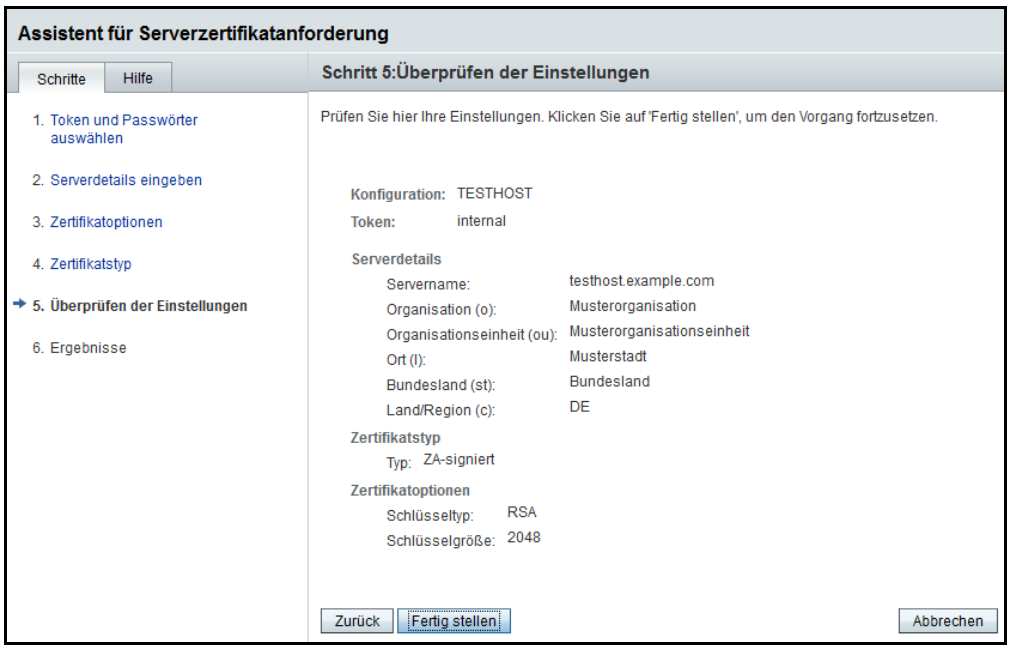
Unter „Schlüsseltyp“ muss der Typ „**RSA**“ ausgewählt werden sowie unter Schlüsselgröße ein Wert von 2048 Bit.
Dies ist der Wert für die Schlüssellänge des Server-Keys und der späteren Zertifikate.
Mögliche Werte sind:
2048 oder 4096.
Empfohlen wird eine Bitlänge von 2048, maximal jedoch 4096 Bit.
Requests mit einer Bitlänge kleiner 2048 Bit gelten nicht länger als sicher und sind von der Beauftragung ausgeschlossen

Abbildung 17



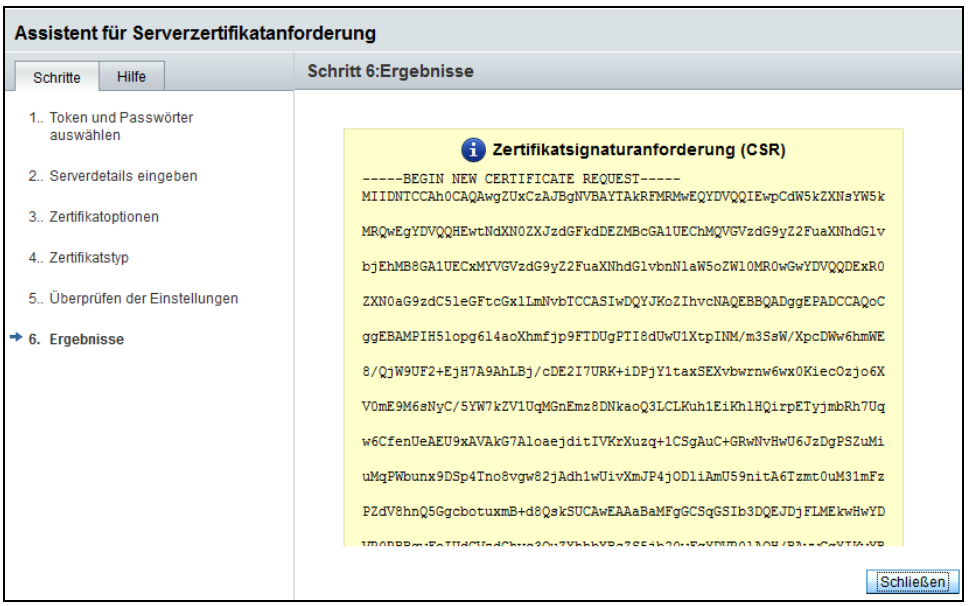
In Abbildung 17 wählen Sie „**ZA-signiertes Zertifikat**“

Abbildung 18



Sind alle Angaben korrekt, kann der Request über „**Fertig stellen**“ erzeugt werden.

Abbildung 19



Der Request wurde erzeugt. Bitte kopieren Sie ihn aus dem Feld unter „Zertifikatsignaturanforderung (CSR)“ incl. der „----BEGIN.... und ----END... “ Zeilen per cut & paste in eine eigene Datei, z. B. zertifikat-requestdatei.txt.
Alternativ lässt sich der Request auch direkt in das entsprechende Feld im Onlineauftrag kopieren.

Abbildung 20 (zertifikat-request.txt)

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

1.1 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-1“ 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 20, inklusive der „----BEGIN.... und ----END... “ Zeilen per cut & paste.

Nach dem Einfügen werden die Request-Inhalte zur Kontrolle angezeigt,
siehe Abbildung 21.

Abbildung 21

Füllen Sie alle weiteren Felder entsprechen Ihren 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.

2.3 Herunterladen und Import der Zertifikate

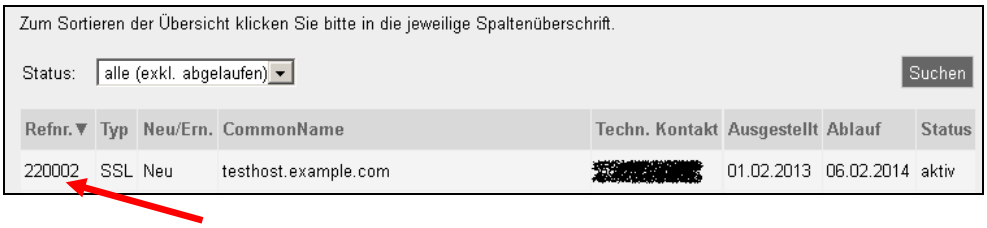
2.3.1 Herunterladen der Zertifikate

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

Wählen Sie den Menüpunkt „Meine Zertifikate“

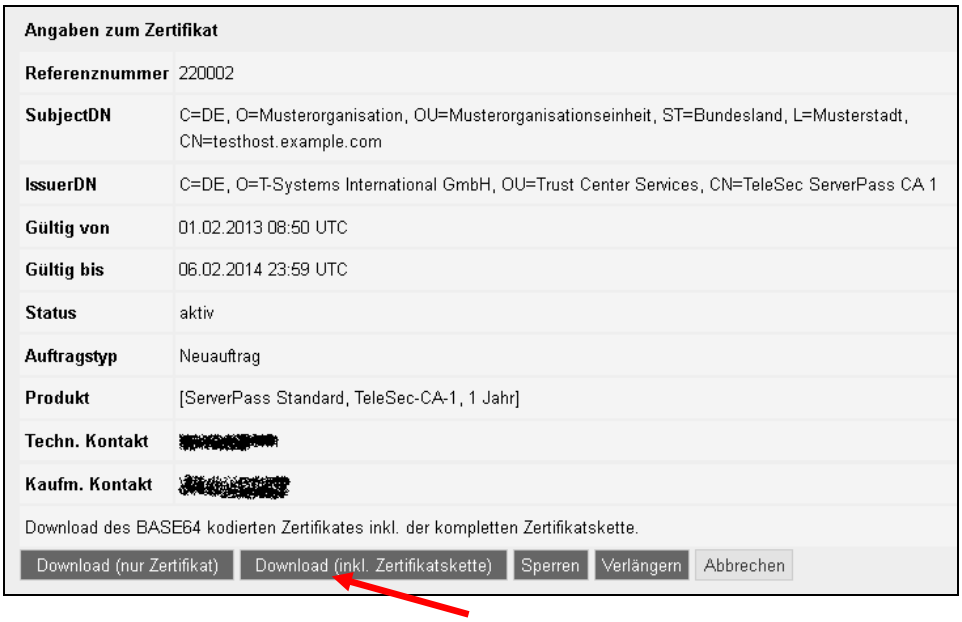
Hier werden nun alle Ihre Zertifikate aufgelistet.

Abbildung 22:



Wählen Sie das herunter zuladende Zertifikat durch Klick auf die Referenznummer aus, siehe Abbildung 22.

Abbildung 23



Es werden zwei Download-Formate angeboten, siehe Abbildung 23:

- Download (Nur Zertifikat)
- Download (inkl. Zertifikatskette)

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

2.3.2 Import der Zertifikate

Öffnen Sie die herunter geladene Datei mit einem einfachen Texteditor z. B. WordPad, ggf. muss bei Öffnen der Dateityp „Alle Dokument *.*“ eingestellt werden.

So wie in Abbildung 24 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 1“, auch CA-Zertifikat genannt.
3. Das Zertifikat „Baltimore CyberTrust Root“ Zertifikat, auch Root-Zertifikat genannt.

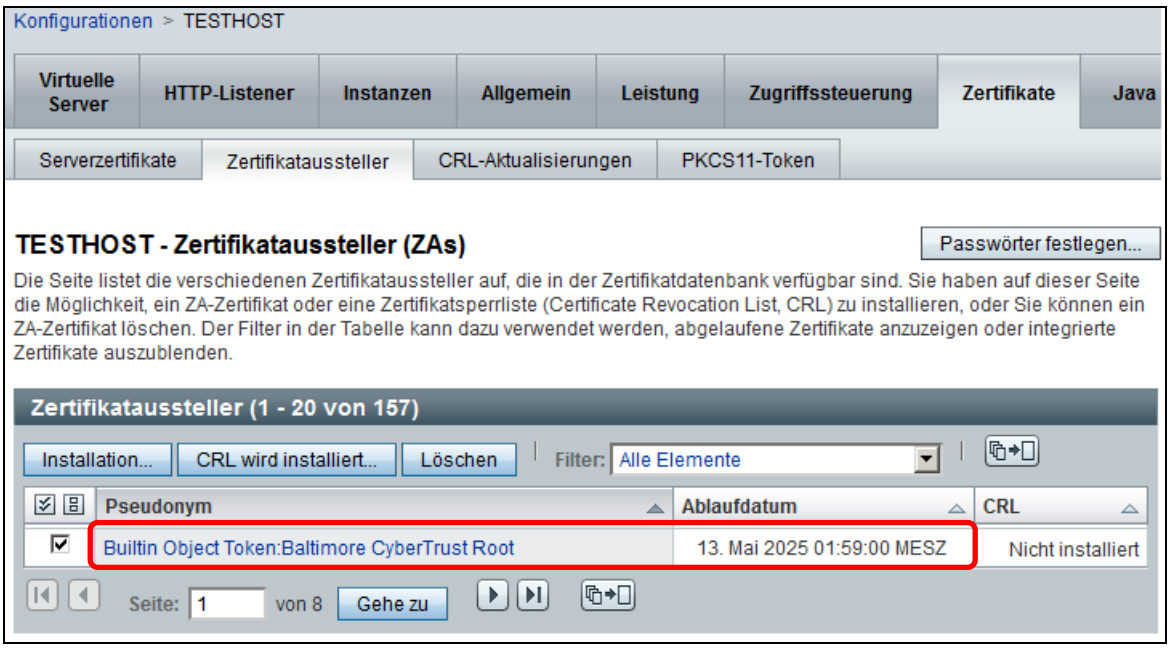
Abbildung 24 (servpass-123456-x509chain.pem)

```
# Ihr ServerPass Zertifikat:
# -------------------------
#   Subject: #   Subject:
C=DE,O=Musterorganisation,OU=Musterorganisationseinheit,ST=Bundesland,L=Musterstadt,
CN=testhost.example.com
#   Issuer: C=DE,O=T-Systems International GmbH,OU=Trust Center Services,CN=TeleSec
ServerPass CA 1
#   Ser.No.: 0x01bce860d56adaec
-----BEGIN CERTIFICATE-----
MIIFxjCCBK6gAwIBAgICQBMwDQYJKoZIhvcNAQEFBQAwgYIxCzAJBgNVBAYTAkRF
...
OGAb1gNE4cu5uYPKtTLbFVyaZ6EhHUoM00Vwl63lU9TUhClrEUZUb5HJ
-----END CERTIFICATE-----
-----# CA Zertifikat:
# CA Zertifikat:
#-------------------------
#   Subject: C=DE,O=T-Systems International GmbH,OU=Trust Center Services,CN=TeleSec
ServerPass CA 1
#   Issuer: C=IE,O=Baltimore,OU=CyberTrust,CN=Baltimore CyberTrust Root
#   Ser.No.: 0x072742c2
-----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-----
```

2.3.3 Prüfen, ob das Root-Zertifikat bereits im Zertifikatsspeicher des Webservers vorhanden ist

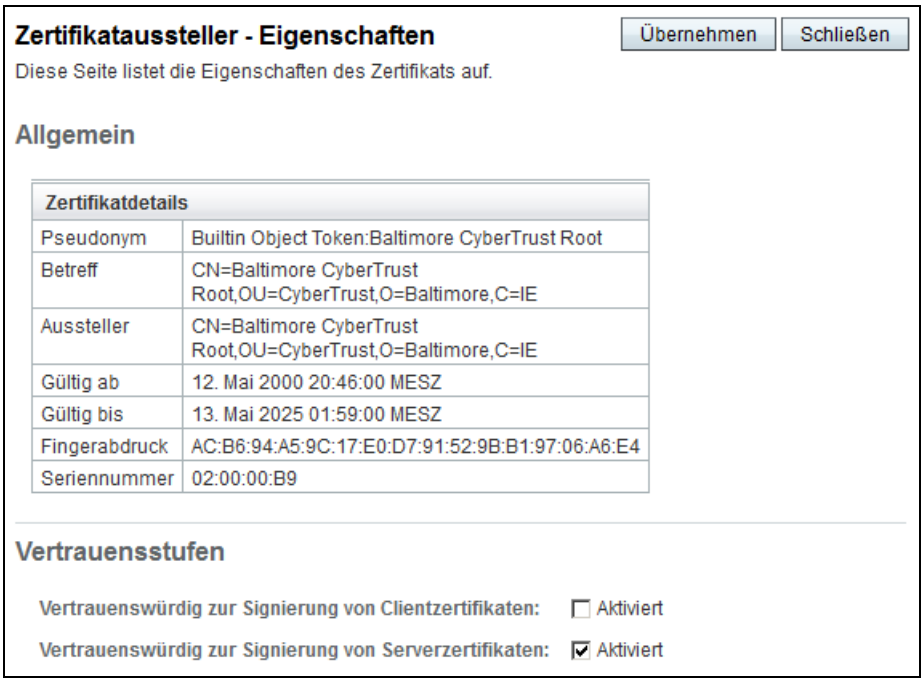
Zur Überprüfung öffnen Sie die Zertifikatsverwaltung, siehe Abbildung 26

Abbildung 26



So wie in Abbildung 26 dargestellt, muss das Zertifikat „Baltimore CyberTrustRoot“ aufgeführt sein. Klicken Sie auf das Zertifikat, um sich die Details anzeigen zu lassen, siehe Abbildung 27.

Abbildung 27



Vergleichen Sie die Zertifikatdetails mit den Einträgen auf unserer Internetseite:

http://www.telesec.de/serverpass/support_rootca_akzeptanz.html -> „Root-CA Zertifikate“

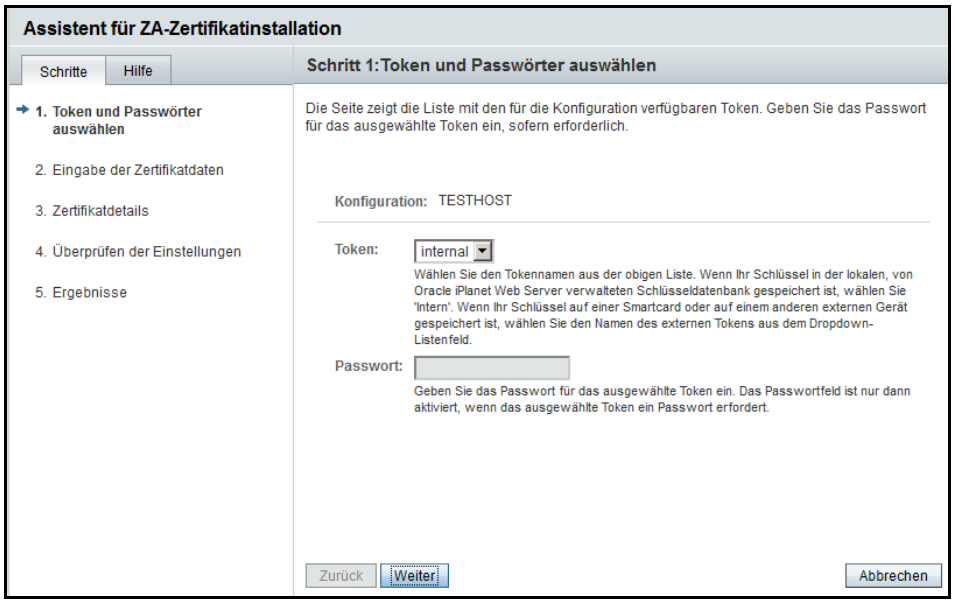
Dieses Zertifikat ist i.d.R. in der Default-Konfiguration enthalten. Wird das Root-Zertifikat nicht aufgeführt, so importieren Sie es gemäß Punkt 2.3.5

2.3.5 ggf. Import des Root-Zertifikat „Baltimore CyberTrust Root“

Wählen Sie im Konfigurationsmenü wieder den Reiter „**Zertifikate**“ gemäß Abbildung 26, anschließend der Reiter „**Zertifikataussteller**“ und den Punkt „**Installation**“ , siehe Abbildung 28.

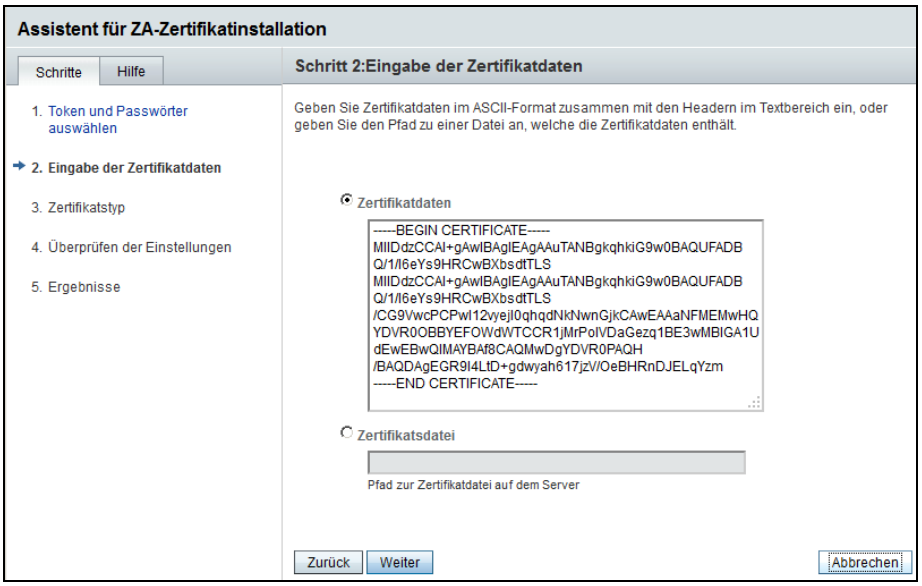
Abbildung 28

Abbildung 29



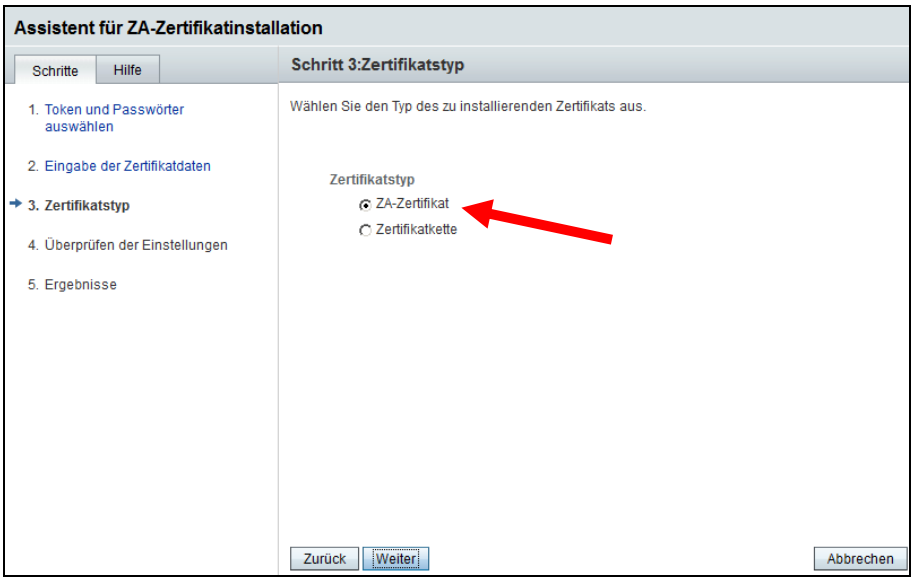
Es öffnet sich der Assistent für ZA-Zertifikatinstallation.
Hier wählen Sie den Token „**internal**“, ggf. ist die Eingabe Ihres Passworts erforderlich.

Abbildung 30



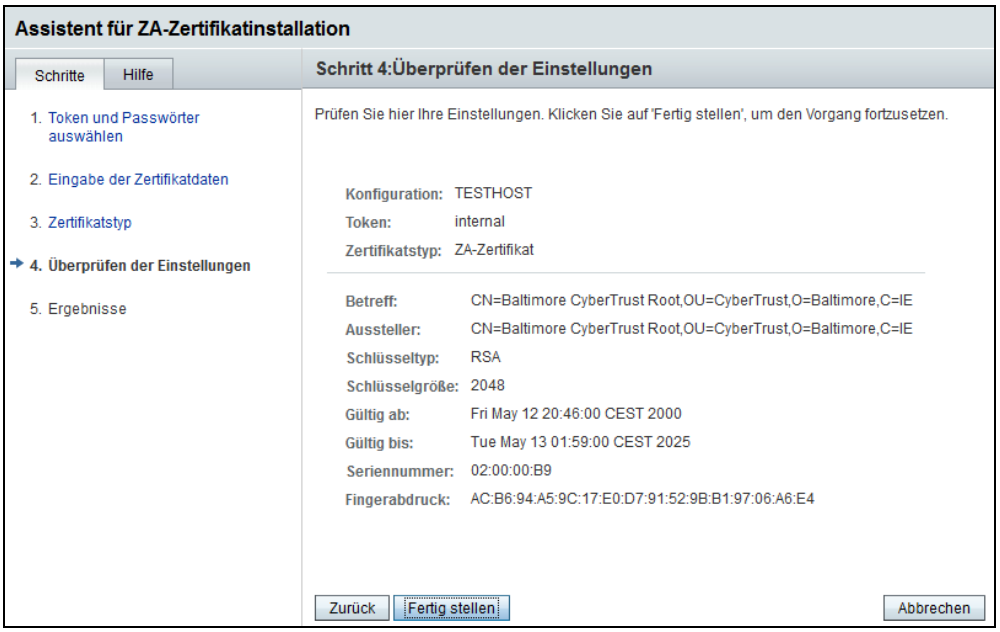
In das Feld „Zertifikatdaten“ kopieren Sie das das Root-Zertifikat „BaltimoreCyberTrustRootCA“ incl. der ---BEGIN... und ---END... Zeilen (grün markiert) aus Abbildung 24.

Abbildung 31



Als Zertifikattyp wählen Sie „**ZA-Zertifikat**“.

Abbildung 32

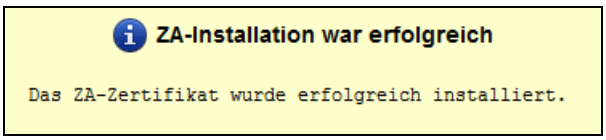


In Abbildung 32 werden alle Details des zu importierenden Zertifikats angegeben. Vergleichen Sie die Details mit den Einträgen auf unserer Internetseite:

https://www.telesec.de/serverpass/ -> Support -> Root-/Sub-CA Zertifikate

Über „Fertig stellen“ wird der Import abgeschlossen.

Abbildung 33



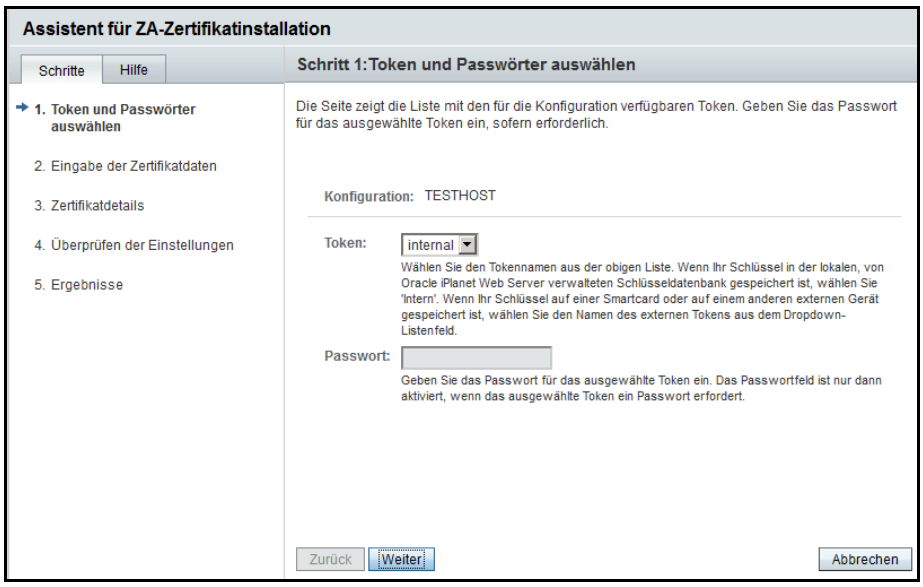
Der erfolgreiche Import wird entsprechend quittiert.

Das Root-CA-Zertifikat wird nun entsprechend Abbildung 26 und 27 aufgelistet

2.3.6 Import des CA-Zertifikats „TeleSec ServerPass CA 1“

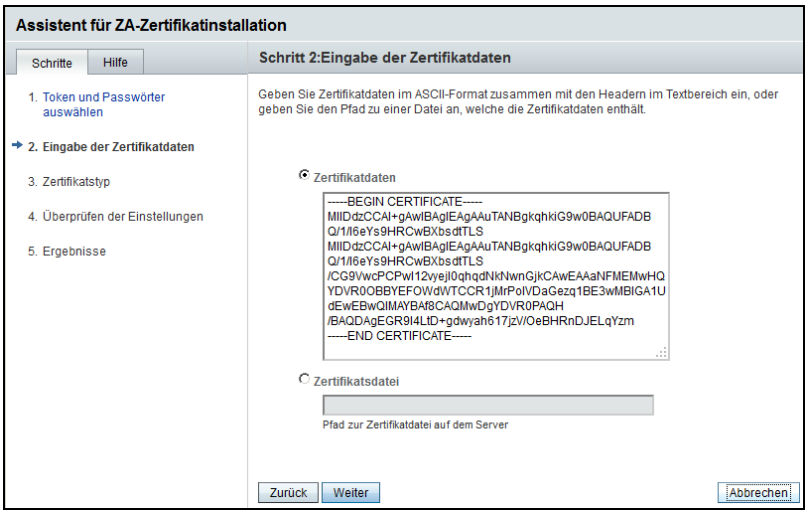
Wählen Sie im Konfigurationsmenü wieder den Reiter „**Zertifikate**“ gemäß Abbildung 26, anschließend der Reiter „**Zertifikataussteller**“ und den Punkt „**Installieren**“, siehe Abbildung 28.

Abbildung 34



Es öffnet sich der Assistent für ZA-Zertifikatinstallation.
Hier wählen Sie den Token „**internal**“, ggf. ist die Eingabe Ihres Passworts erforderlich.

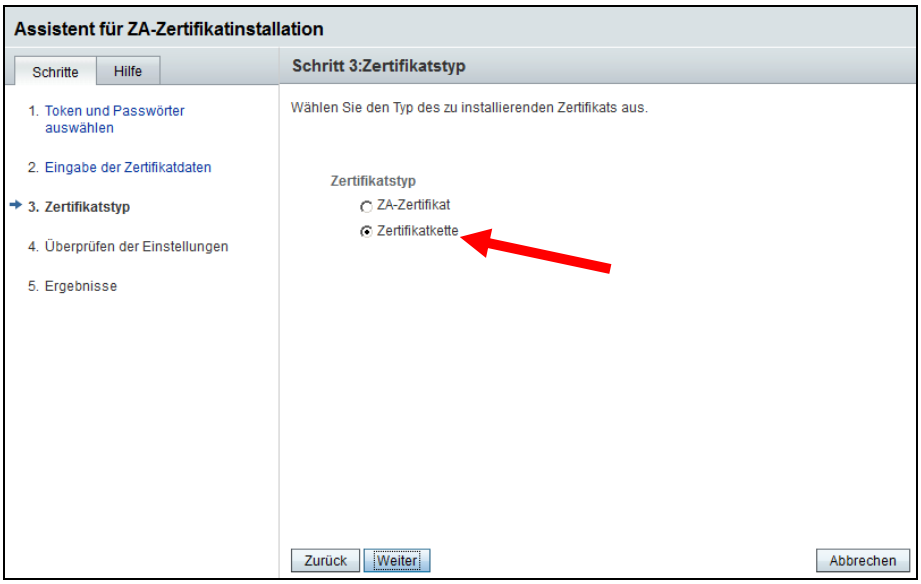
Abbildung 35



In das Feld „Zertifikatdaten“ kopieren Sie das das CA-Zertifikat

„TeleSec ServerPass CA 1“ incl. der ---BEGIN... und ---END... Zeilen (magenta markiert) aus Abbildung 24.

Abbildung 36



Als Zertifikattyp wählen Sie „**Zertifikatkette**“.

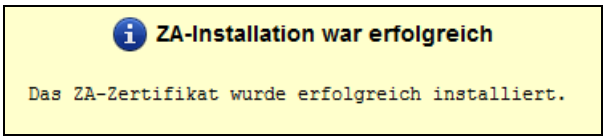
Abbildung 37

In Abbildung 37 werden alle Details des zu importierenden Zertifikats angegeben. Vergleichen Sie die Details mit den Einträgen auf unserer Internetseite:

https://www.telesec.de/serverpass/ -> Support -> Root-/Sub-CA Zertifikate

Über „**Fertig stellen**“ wird der Import abgeschlossen.

Abbildung 38



Der erfolgreiche Import wird entsprechend quittiert.

Das CA-Zertifikat wird nun entsprechend Abbildung 39 aufgelistet.

Abbildung 39

Durch einen Klick auf das Zertifikat lassen sich die Zertifikatdetails anzeigen.

2.4 Installation des Serverzertifikats

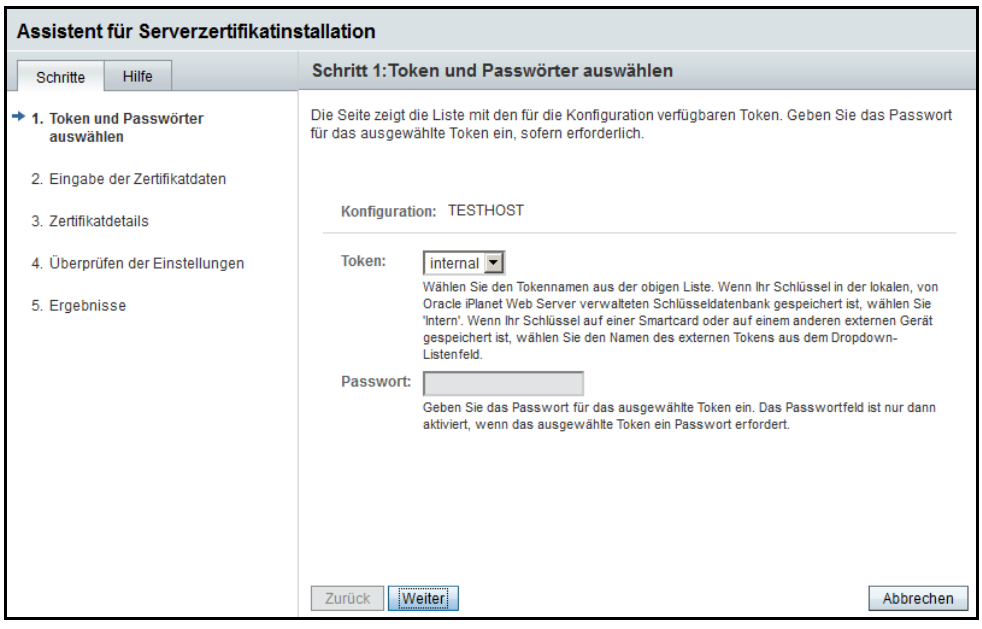
Nun erfolgt der Import des Serverzertifikats

Öffnen Sie die Konfiguration des Virtuellen Servers und wählen den Reiter „**Serverzertifikate**“, siehe Abbildung 40.

Abbildung 40

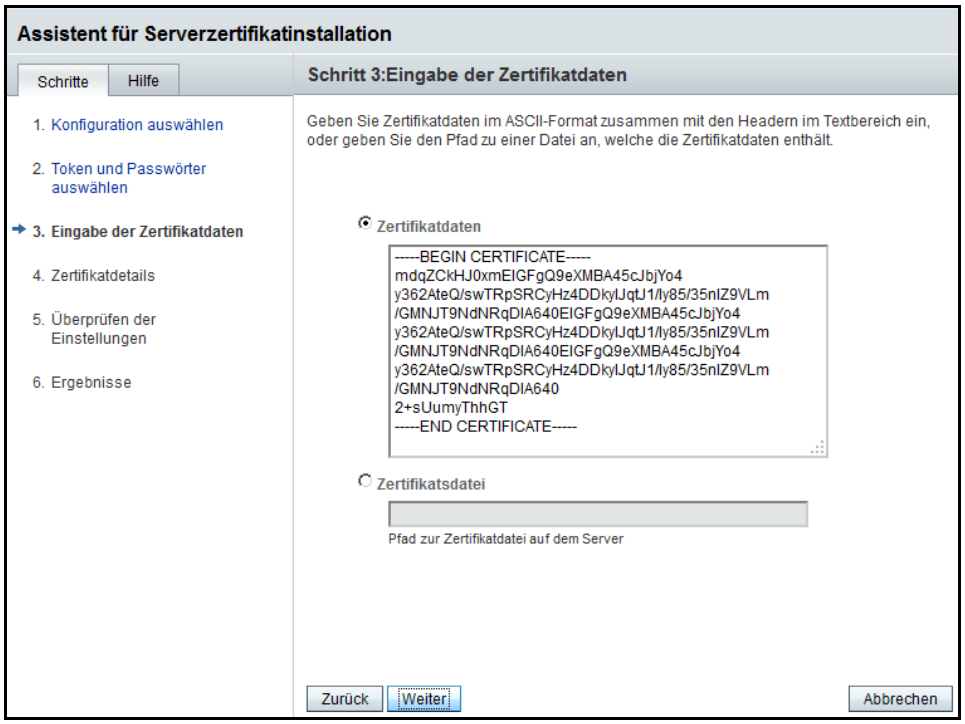
In Abbildung 40 wählen Sie „**Installation**“, ggf. ist die Angabe Ihres Passworts erforderlich.

Abbildung 41



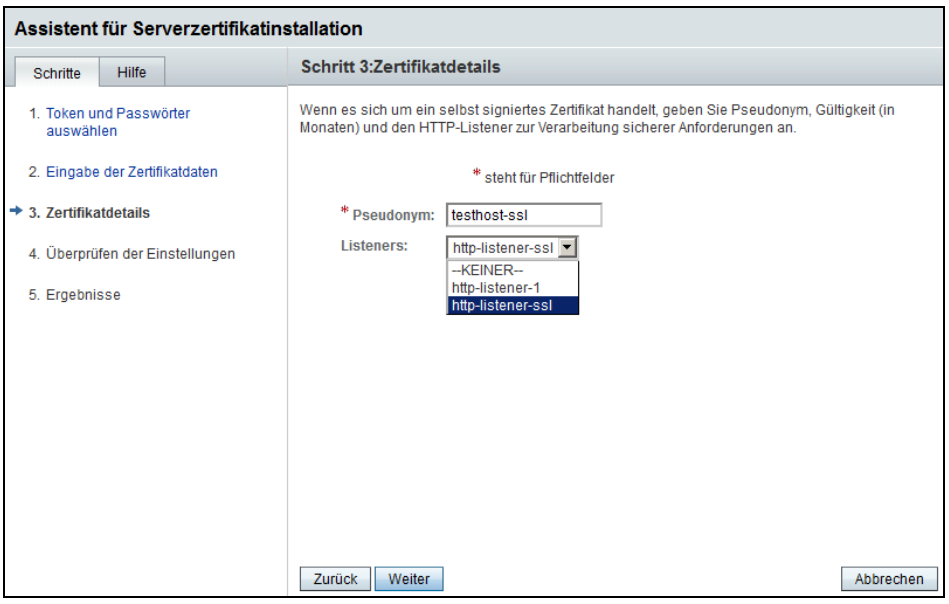
Hier wählen Sie den Token „**internal**“, ggf. ist die Eingabe Ihres Passworts erforderlich.

Abbildung 42



In das Feld „Zertifikatdaten“ kopieren Sie das Zertifikat „**Ihr ServerPass Zertifikat**“ incl. der ---BEGIN... und ---END... Zeilen (blau markiert)
aus Abbildung 24.

Abbildung 43



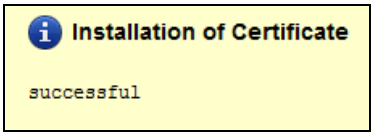
Für das zu importierende Serverzertifikat muss ein Pseudonym vergeben werden, z. B. testhost-ssl.

Auch muss das Zertifikat an den HTTP-Listener gebunden werden, der für den SSL-Modus vorgesehen ist. Im Beispiel ist dies „http-listener-ssl“.

Abbildung 44

In Abbildung 44 werden die Details Ihres Serverzertifikats dargestellt.
Überprüfen Sie die Angaben und schließen den Import über „**Fertig stellen**“ ab.

Abbildung 45



Der erfolgreiche Import wird entsprechend quittiert.

Abbildung 46

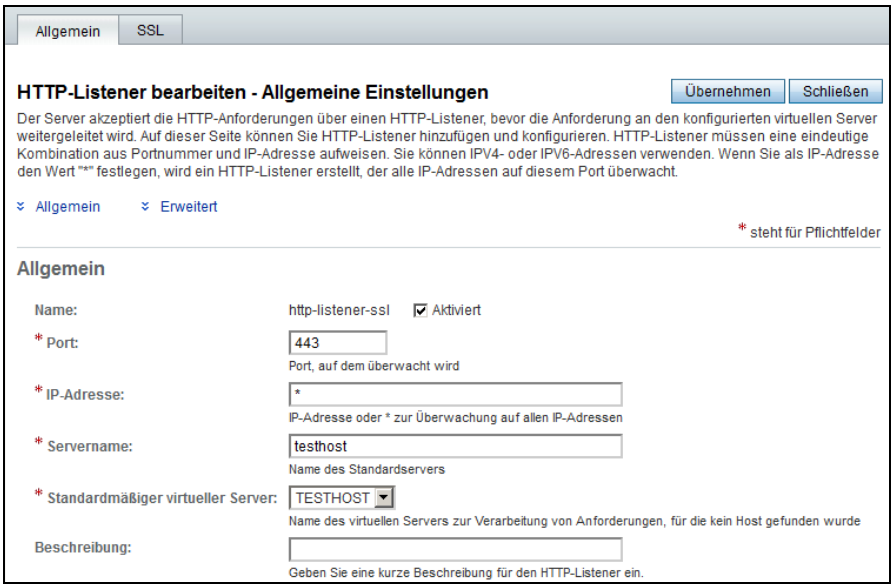
So wie in Abbildung 46 gezeigt, wird das importierte Zertifikat nun unter „Serverzertifikate“ aufgelistet.

Nun muss des SSL-Modus aktiviert werden.
Wählen Sie hierfür den Reiter „**HTTP-Listener**“, siehe Abbildung 47.

Abbildung 47

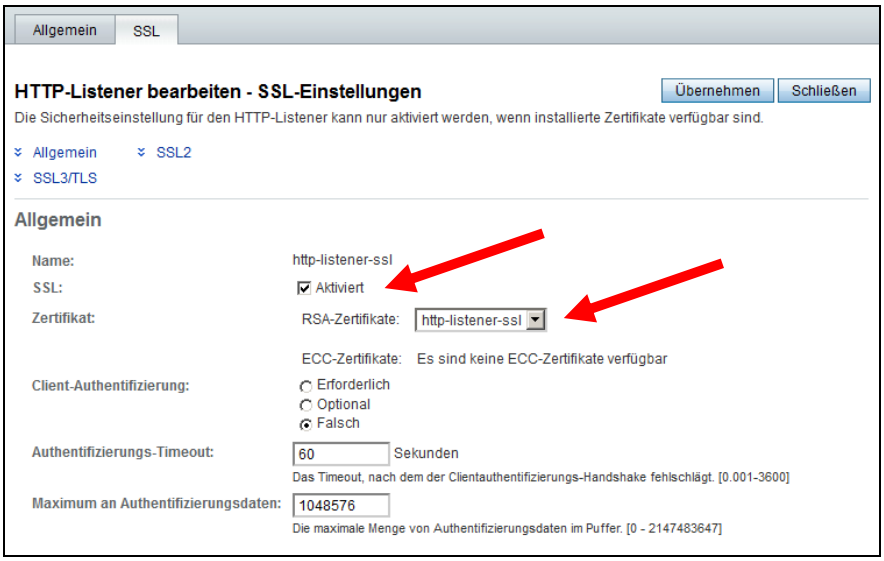
Falls wie in Abbildung 47 dargestellt, der SSL-Modus für den Listener „http-listener-ssl“ auf „deaktiviert“ steht, muss der SSL-Modus aktiviert werden. Wählen Sie den für SSL vorgesehenen HTTP-Listener aus, im Beispiel ist dies „http-listener-ssl“.

Abbildung 48



In der Konfiguration „HTTP-Listener bearbeiten“ wählen Sie den Reiter „Allgemein“ und aktivieren die Option „htt-listener-ssl“. Als Port wird standartmäßig Port „443“ verwendet. Alle anderen Angaben wählen Sie entsprechend Ihrer Konfiguration aus und übernehmen die Einstellungen.
Über den Reiter „**SSL**“ lassen sich die Optionen für den SSL-Modus konfigurieren, siehe Abbildung 49.

Abbildung 49



Gemäß Abbildung 49 wird der SSL-Modus aktiviert und der zu verwendende http-Listener ausgewählt. Im Beispiel ist dies „http-listener-ssl“.
Wählen Sie die übrigen Optionen gemäß Ihren Vorgaben aus und übernehmen die Änderungen über den entsprechenden Button.

Abbildung 50

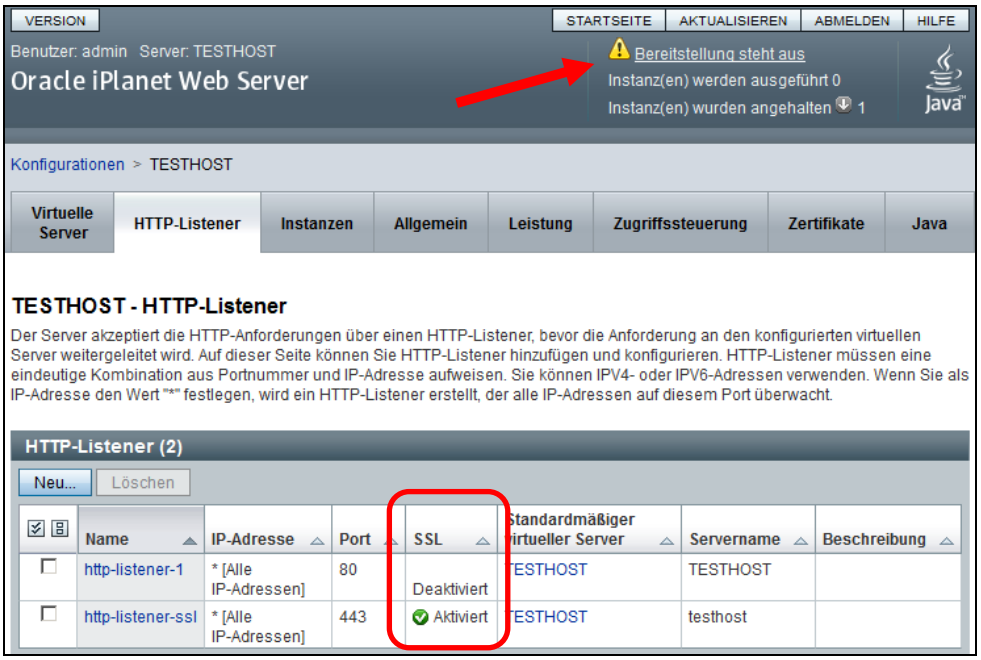
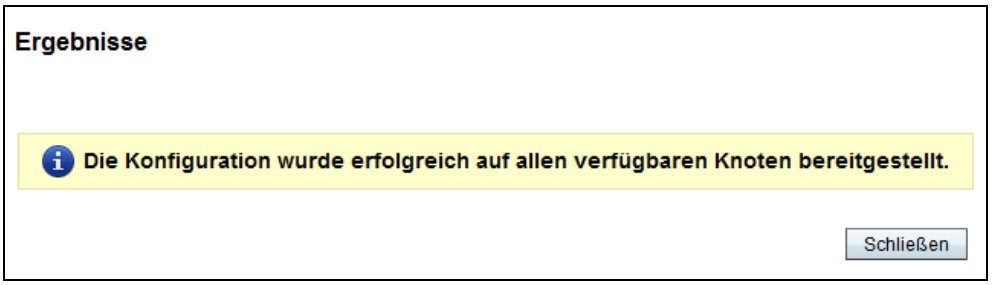


Abbildung 50 zeigt den aktivierten SSL-Modus.
Abschließend muss die Konfiguration noch „bereitgestellt“ werden. Dies geschieht über den entsprechenden Button oben rechts - „**Bereitstellung steht aus**“.

Abbildung 51

Über „**Bereitstellen…**“ werden die Änderungen übernommen.

Abbildung 52



Die Erfolgreiche Übernahme der Änderung wird entsprechend quittiert.
Sie können das Fenster schließen.

Die Installation ist Abgeschlossen.

2.5 Sicherung der Dateien

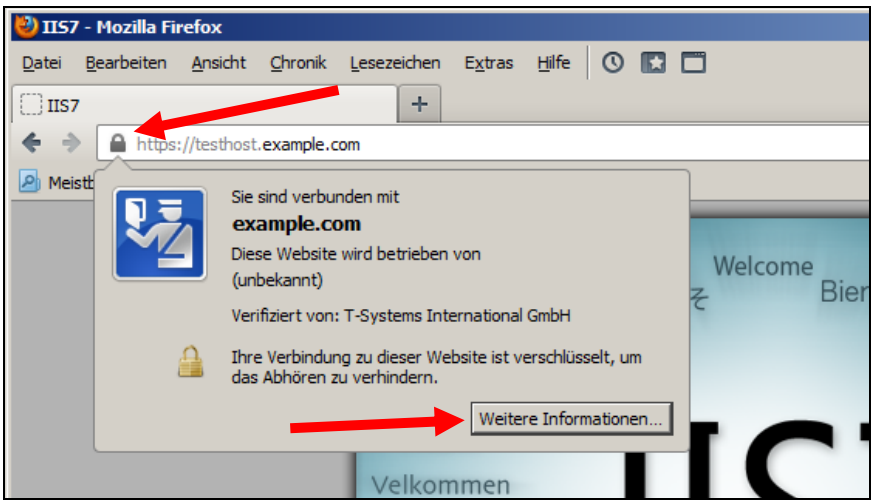
Es wird dringend empfohlen, die erzeugten Dateien zu sichern, z. B. auf einem externen Medium!
Gesichert werden sollten die Schlüssel-Dateien des virtuellen Hosts, „cert8.db“, „key3.db“. und „secmod.db“. In der Beispielkonfiguration befinden sie sich unter:
C:\Program Files\Oracle\WebServer7\https-TESTHOST\config\

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 53-55) sowie im Internet Explorer (Abbildung 56-58) aufgeführt.

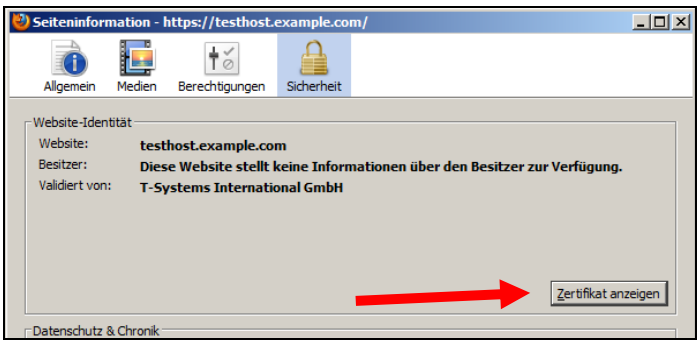
Firefox:

Abbildung 53 (Firefox 18):



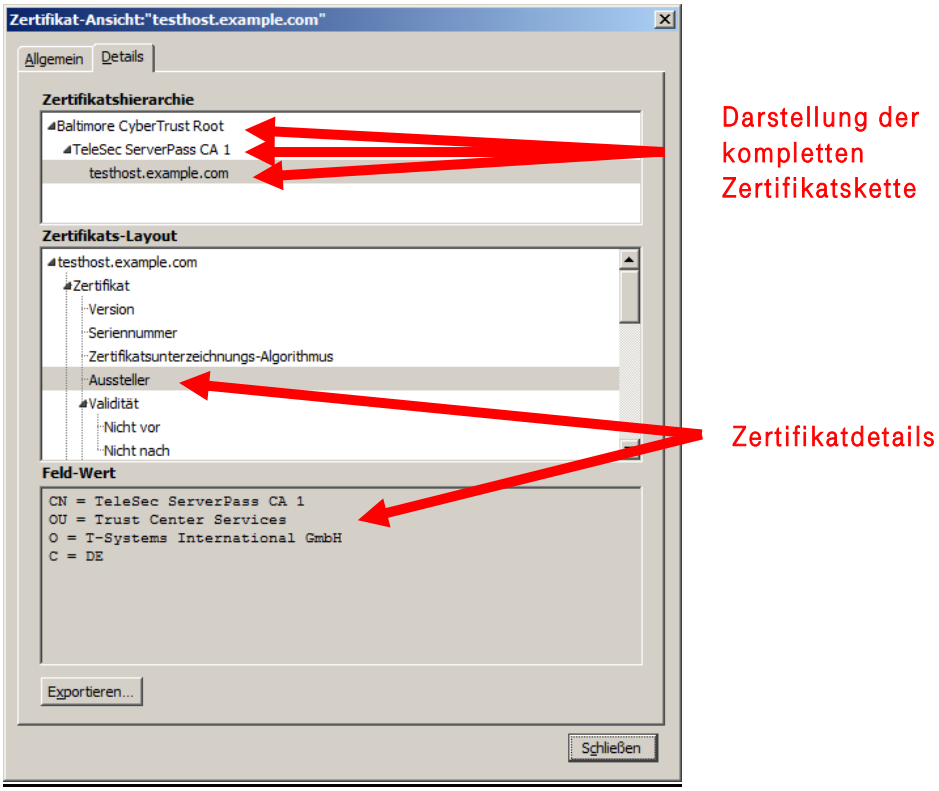
Beim Firefox lassen sich über einen Klick auf das Schloss Details zum verwendeten Zertifikat anzeigen.
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 54 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

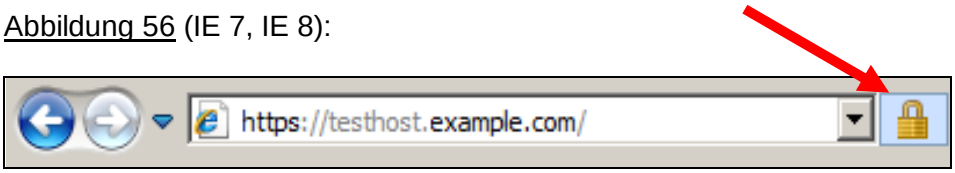
Abbildung 55 (Firefox 18):



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“

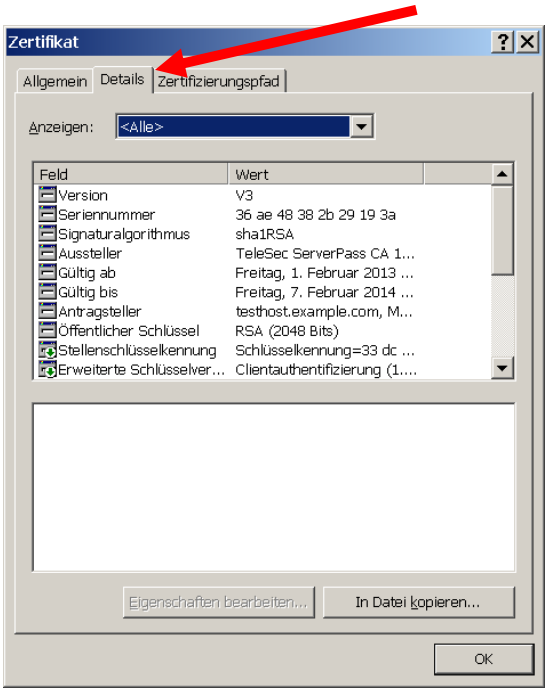
Internet Explorer

Abbildung 56 (IE 7, IE 8):



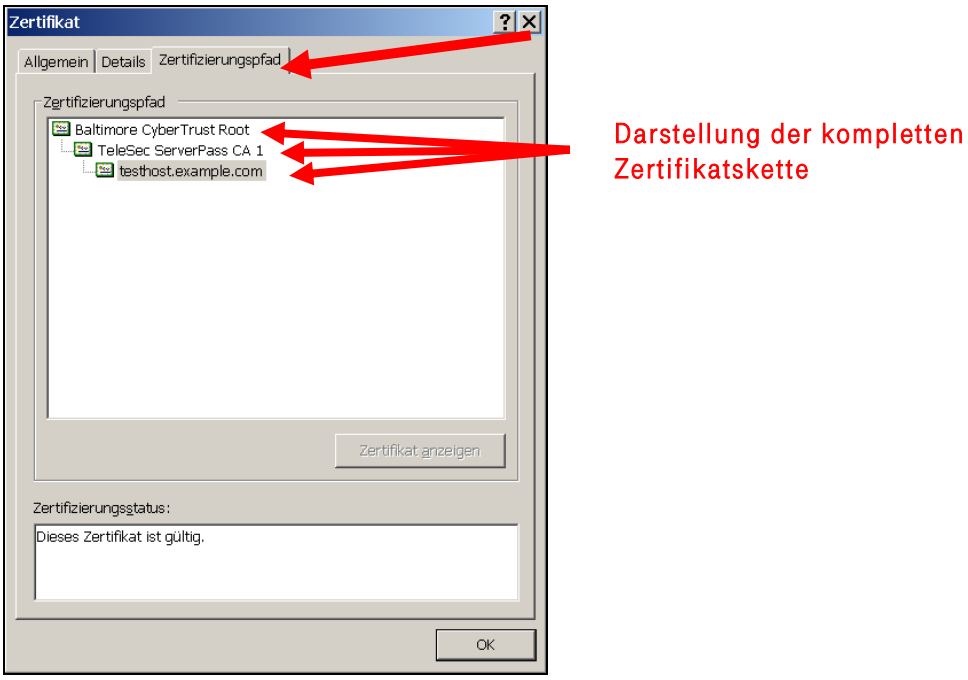
Beim Internet Explorer lassen sich die Zertifikatsdetails durch Doppelklick auf das Schloss anzeigen.
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 57.

Abbildung 57 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 14.

Abbildung 58 (Die Zertifikatskette)



So wie in Abbildung 58 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.