TeleSec ServerPass

Zertifikats-Erneuerung 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_erneu_inst_oracle_iplanet_7_webserver.doc		Zertifikats-Erneuerung Oracle iPlanet 7 Webserver

Version	Stand	Status
1.1	14.04.2014	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
Zertifikat Erneuerung 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 Zertifikatserneuerung 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.

Für eine Erneuerung halten Sie bitte das Service-Passwort des zu erneuernden Zertifikats bereit, da es im Zuge der Beauftragung abgefragt wird.

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 läuft bereits im SSL-Modus unter Verwendung eines TeleSec ServerPass Serverzertifikats.
Die „ausstellenden Instanzen“ (CA- und ggf. Root-Zertifikat) für TeleSec ServerPass wurden bereits korrekt installiert.
Sollten diese Zertifikate noch nicht installiert sein, so installieren Sie diese bitte vorab gemäß Anleitung „Oracle iPlanet 7 Webserver -> Zertifikat-Requesterzeugung, Installation der Zertifikate“.

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

2 Zertifikat erneuern

2.1 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 Kundeportal myServerPass.

Achtung: eine nochmalige Verwendung eines bereits für eine Beauftragung verwendeten Server-Schlüssels ist nicht zulässig.
Daher ist ggf. die Erzeugung eines neuen Zertifikat-Requests erforderlich. Folgen Sie hierzu bitte der Anleitung „Oracle iPlanet 7 Webserver -> Zertifikat-Requesterzeugung, Installation der Zertifikate“.

2.2 Besonderer Hinweis für eine Zertifikats-Erneuerung mit Oracle iPlanet 7 Webserver

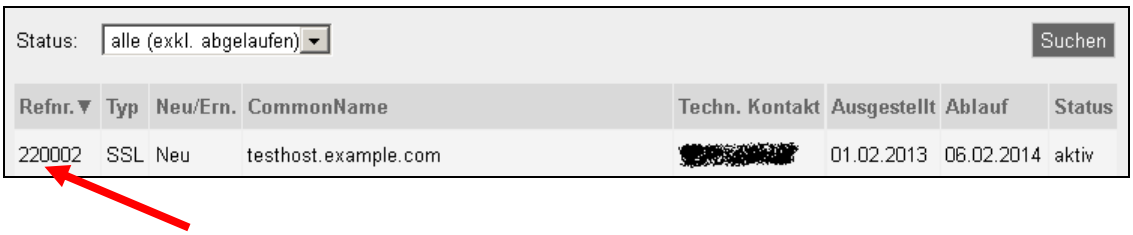
In der Regel ist die Erzeugung eines weiteren Requests nicht erforderlich.
Sollte dennoch ein neuer Request erzeugt werden, so erzeugen Sie bitte eine neue Zertifikatsanforderung, gemäß Anleitung „„Oracle iPlanet 7 Webserver -> Zertifikat-Requesterzeugung, Installation der Zertifikate“.
Beachten Sie, dass während der Requesterzeugung die gleichen Angaben (Organisation, Organisationseinheit, Common Name, Stadt, Bundesland, Staat, evtl. auch Strasse und Postleitzahl) gemacht werden müssen, wie bei der Beauftragung des zu erneuernden TeleSec ServerPass Zertifikats. Ansonsten können Sie die Erneuerungsfunktion im Webportal „MyServerPass“ nicht nutzen.
Die Angaben des zu erneuernden Zertifikates lassen sich z. B. im Servermanager anschauen. Dieser Vorgang wird in der Anleitung beschrieben.

Der Webserver läuft bis zum Import des neuen Zertifikats mit dem bestehenden Zertifikat weiter.

2.3 Erneuerung durchführen

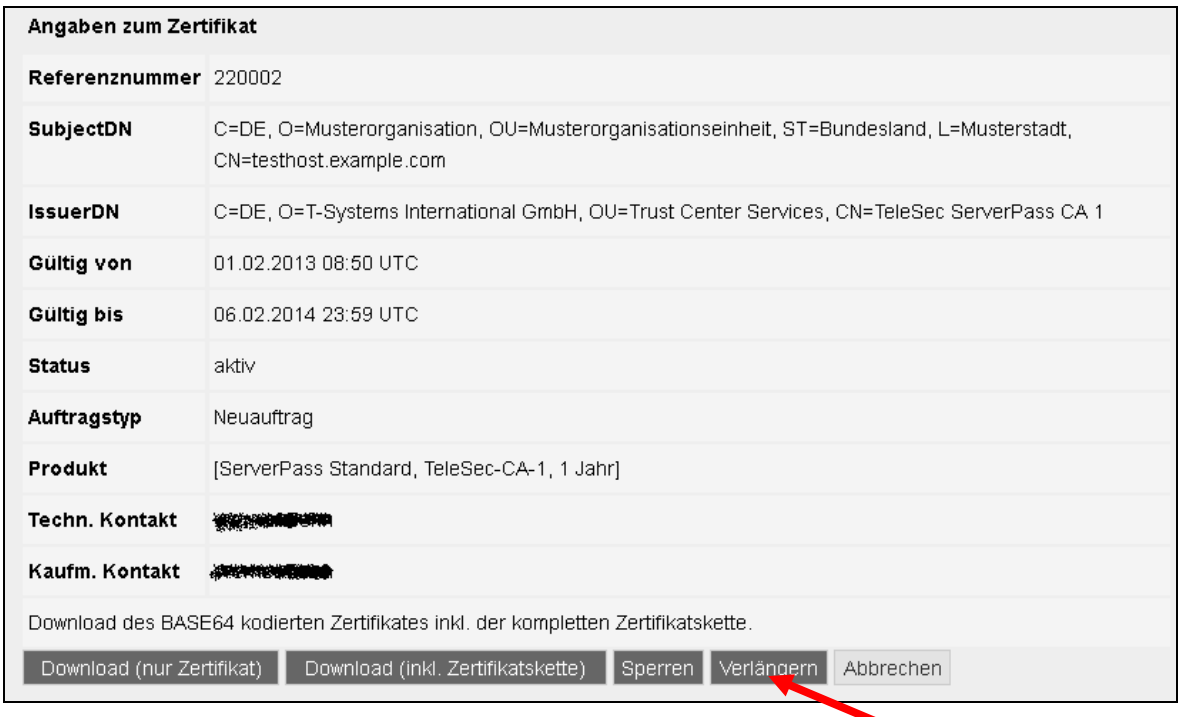
Melden Sie sich am Kundenportal „myServerPass“ an.
Unter dem Menüpunkt “Meine Zertifikate“ erscheint eine Liste aller Ihrer Zertifikate, siehe Abbildung 1.
Hier können Sie nun das zu erneuernde Zertifikat anhand der Referenznummer ermitteln.
Die Zertifikatseinträge lassen sich durch Klicken auf die „Referenznummer“ oder den „Common Name“ anzeigen.

Abbildung 1 (Ausschnitt des Kundenportals):



Durch Klicken auf die Referenznummer lassen sich die Zertifikatdetails anzeigen.

Abbildung 3: (Zertifikatdetails)



Über „Abbrechen“ können Sie zur Liste zurückkehren.
Haben Sie das korrekte Zertifikat ermittelt, wählen Sie den Button „Verlängern“.
Anschließend bekommt man die Zertifikatsdaten des zu erneuernden Zertifikats angezeigt.
Treffen Sie die gewünschte Root- sowie Produkt-Auswahl (Laufzeit).
Ggf. muss ein neues Produkt ausgewählt werden, z. B. wenn das ausstellende Zertifikat geändert wurde, siehe Abbildung 4.

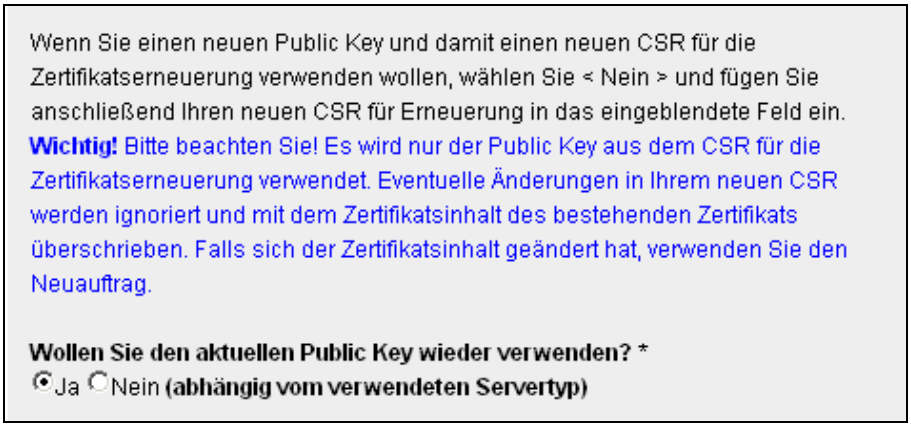
Abbildung 4:

Anschließend wird die Verwendung des Public Keys abgefragt, siehe Abbildung 5.

2.3.0 Die Verwendung des Public Keys bei der Erneuerung

Bei einer Erneuerung stehen zwei Optionen zur Auswahl, siehe Abbildung 5:

Abbildung 5: (Verwendung des Public Keys)



2.3.1 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.
Das Zertifikat wird i. d. R. sofort und ohne weitere Nachfrage ausgestellt und steht zum Download bereit. Hierzu klicken Sie auf die „ServerPass herunterladen“.

2.3.2 Erneuerung unter Verwendung eines neuen Public Keys

Steht der private Schlüssel des zu verlängernden Zertifikats nicht mehr zur Verfügung, muss zunächst ein neuer Schlüssel bzw. ein neuer Request erzeugt werden.

Die Vorgehensweise wird erläutert in der Anleitung „Oracle iPlanet 7 Webserver -> Zertifikat-Requesterzeugung, Installation der Zertifikate“.

Die Feldeinträge (Common Name, Locality, Country usw.) des zu erzeugenden Request müssen exakt dem zu erneuernden Zertifikat entsprechen.
Diese Einträge lassen sich z. B. im Kundenportal myServerPass ermitteln.

Melden Sie sich am Kundenportal „myServerPass“ an.
Unter dem Menüpunkt “Meine Zertifikate“ erscheint eine Liste aller Ihrer Zertifikate, siehe Abbildung 1.

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. Wichtig sind die Angaben für „SubjectDN“, siehe Abbildung 6.
Abbildung 6: (Zertifikatsdetails)

Angaben zum Zertifikat	
Referenznummer	220002
SubjectDN	C=DE, O=Musterorganisation, OU=Musterorganisationseinheit, ST=Bundesland, L=Musterstadt, CN=testhost.example.com
IssuerDN	C=DE, O=T-Systems International GmbH, OU=Trust Center Services, CN=TeleSec ServerPass CA 1
Gültig von	01.02.2013 08:50 UTC
Gültig bis	06.02.2014 23:59 UTC
Status	aktiv

Nun muss ein neuer Request unter Berücksichtigung der hier ermittelten Daten erzeugt werden.

Die Erzeugung eines Serverschlüssels sowie eines Zertifikatrequests wird beschrieben in der Anleitung „Microsoft Internet Information Server (IIS) V7.0“ → „Zertifikat-Requesterzeugung, Installation der Zertifikate“.

Sobald der neue Request für die Erneuerung vorliegt, so wählen Sie bei der Frage „Wollen Sie den aktuellen Public Key wieder verwenden?“ die Option „Nein“ und kopieren den 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 7.

Abbildung 7: Request-Prüfung

Bitte überprüfen Sie nach dem Einfügen des Requests die angezeigten Inhalte.

Mein PKCS#10 Zertifikats-Request *

```
AjALBglghkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFGCn
BZgKDIBRRd5RDtejtu8UVri1MA0GCSqGSIb3DQEBBQUAA4IBAQDRRifAIKxLmH8r
hXFXNtgF33ABSq4OcmTNWMhle+f1wHQ9D2TuJKt2v4LVET8WCtkF23E9XI9OO9gb
nXQf9VWHfnbqbOsD/7AKnno9X9TmEzA7mkGe4khRH8vccPeTP+aDFuA5r6ojT95p
mxxlJ7qsvSQ17QI/mEDc5xL6/AZ/DUKI2s28uQjVAgIfct/zd8a0GrgyHzE+ztJ3
ZZDJiqsOYJWpwWq0vpBXmP7I1RnJ+b3jNBfYf2xyiaI9umMDYbyMjoSTY7xve42D
wCKGkw/OD6YhUoQsQTW1fkwVBM1kUz4rqYiIA+cE2/510S1JvMYPIT0JU/cmn4IV
sMp1uF/2
-----END NEW CERTIFICATE REQUEST-----
```

Ihr Zertifikats-Request wurde untersucht und enthält den nachfolgenden Inhalt:

CN:	**testhost.example.com**
C:	DE
O:	Musterorganisation
OU1:	Musterorganisationseinheit
ST:	Bundesland
L:	Musterstadt
SAN 1(=CN):	testhost.example.com

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.

Nun werden alle weiteren Angaben (Produktauswahl, Laufzeit, Identifikationsangaben, Servicepasswort des zu verlängernden Zertifikats usw.) entsprechend Ihrer Vorgaben ausgewählt und der Auftrag abgeschickt.

Das Zertifikat wird i. d. R. sofort und ohne weitere Nachfrage ausgestellt und steht zum Download bereit. Hierzu klicken Sie auf die „ServerPass herunterladen“.

2.4 Import des erneuerten Zertifikats

2.4.1 Herunterladen des erneuerten Zertifikats

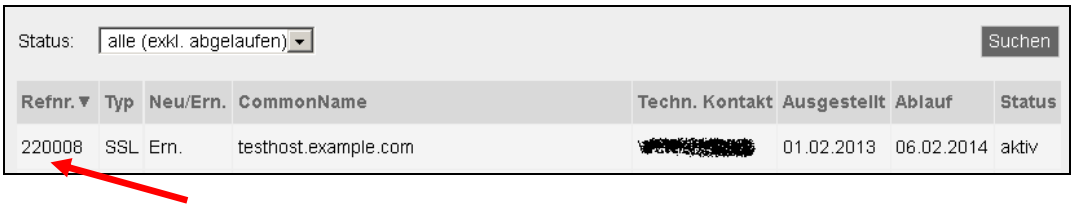
Wie beschrieben, lässt sich das Zertifikat aus dem vorangegangen Dialog herunterladen bzw. erst nach Anmeldung im Portal „myServerPass“:

www.telesec.de/serverpass/index.html (→ myServerPass)

Wählen Sie den Menüpunkt „Meine Zertifikate“

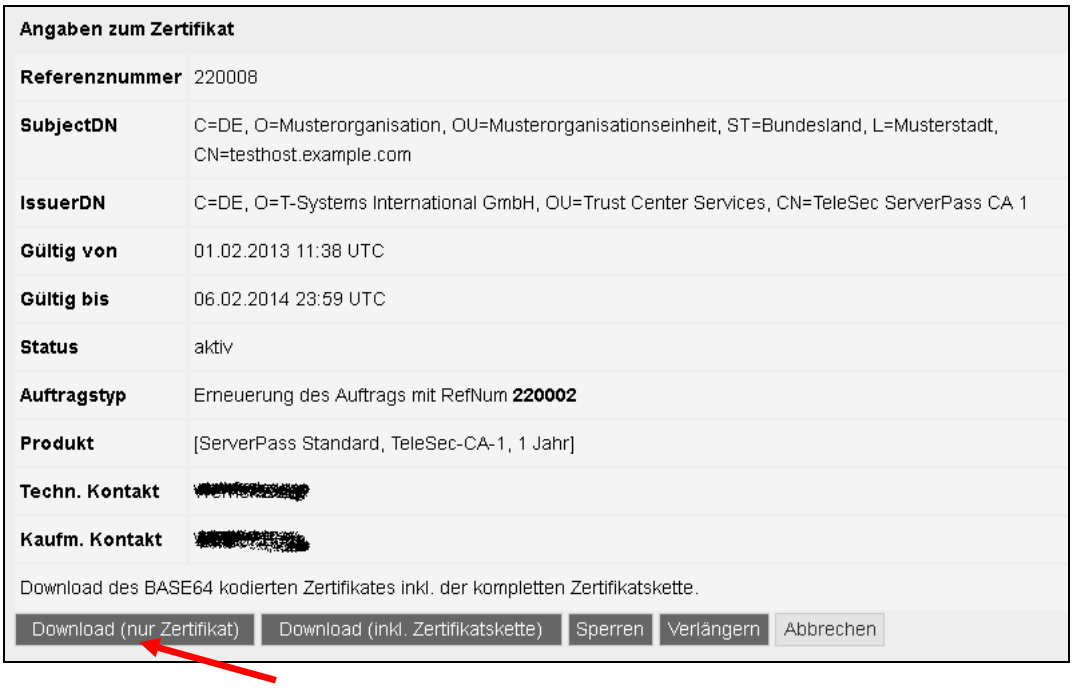
Hier werden nun alle Ihre Zertifikate aufgelistet, siehe Abbildung 8.

Abbildung 8



Wählen Sie das herunter zuladende Zertifikat durch Klick auf die Referenznummer aus.

Abbildung 9



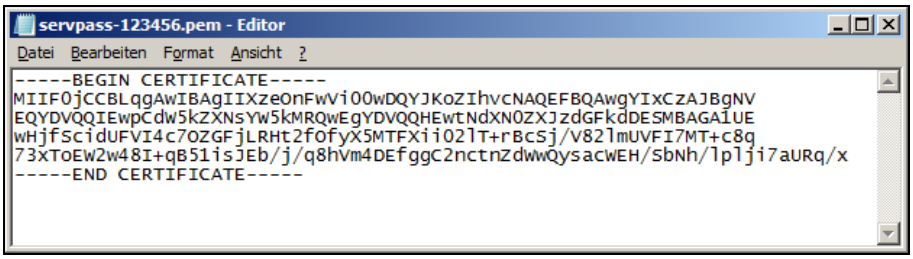
Wie in Abbildung 9 gezeigt, werden die Zertifikatsdaten zur Kontrolle angezeigt.
Angeboten werden zwei Download-Formate:

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

Wählen Sie das Format: „Download nur das Zertifikat“.
Aktivieren Sie die Option „Als Datei speichern und legen einen Dateipfad fest, z. B. c:\
Sie erhalten die Datei „servpass-123456.pem“ und sie liegt nun unter c:\.

Die herunter geladene Datei enthält das Server-Zertifikat, wie in Abbildung 10 dargestellt.

Abbildung 10 (servpass-123456.pem)



2.4.2 Import des Serverzertifikats

Öffnen Sie die Konfiguration Console des Oracle iPlanet 7 Webservers,

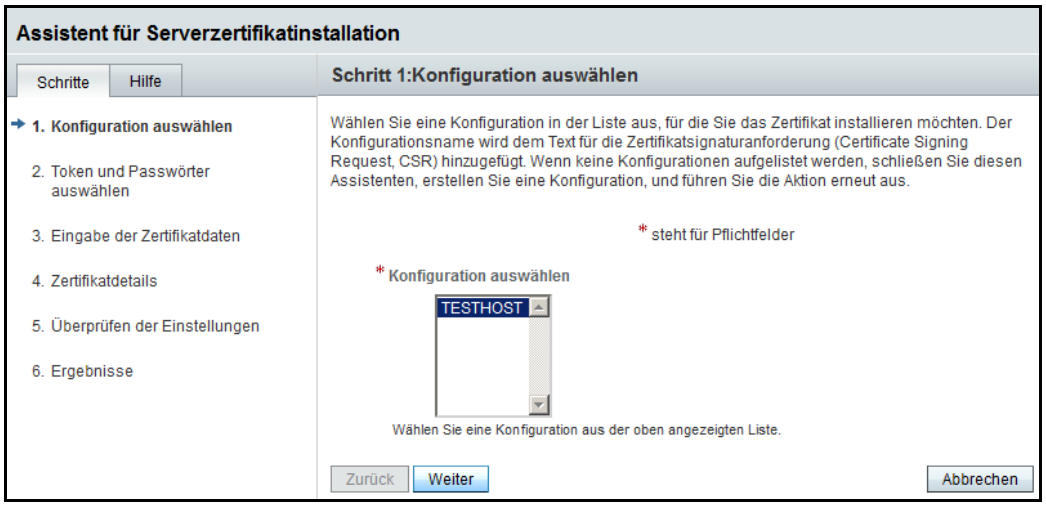
siehe Abbildung 11.

In dieser Anleitung wird kein Passwort zum Schutz der Zertifikate vergeben.
Wurde ein Passwort definiert, so muss es bei den nachfolgenden Aktionen immer wieder eingegeben werden.

Abbildung 11

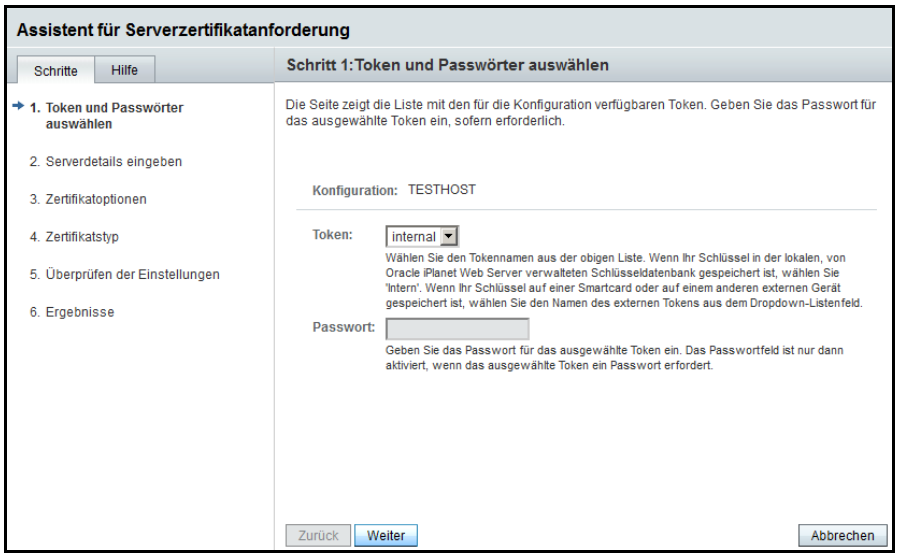
Wählen Sie den Menüpunkt „Serverzertifikat installieren“.
Es öffnet sich der Assistent für die Serverzertifikatinstallation, siehe Abbildung 12.

Abbildung12



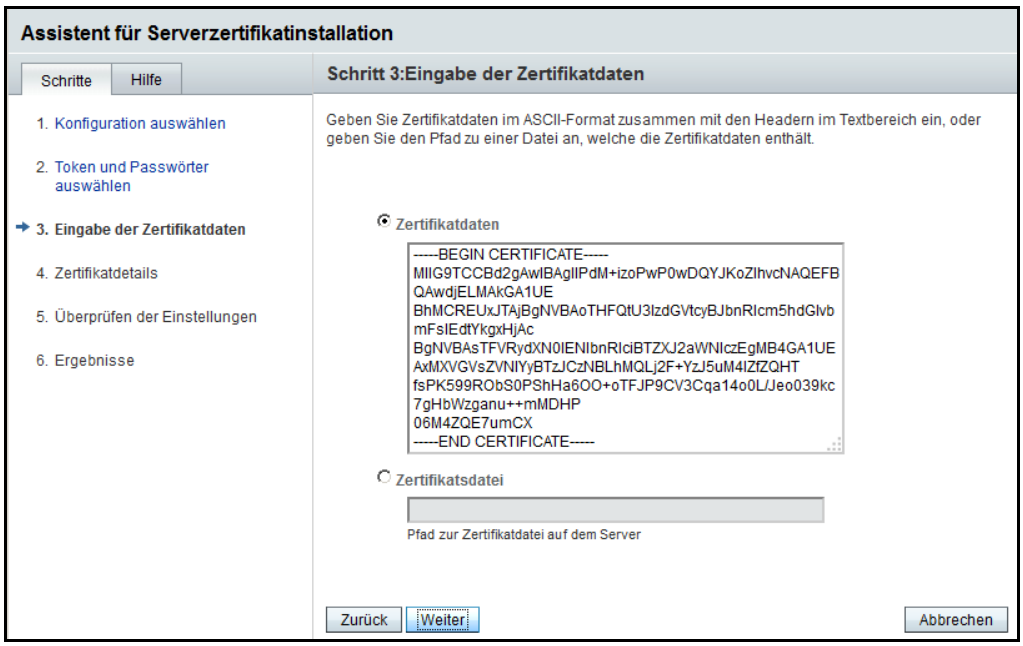
Wählen Sie Ihre Konfiguration aus.

Abbildung 13



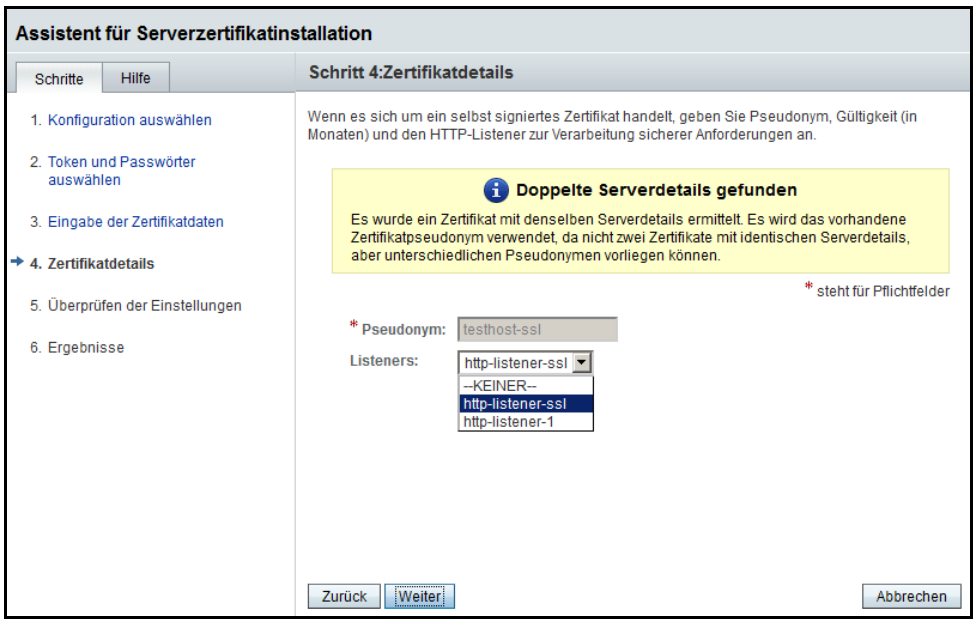
Wählen Sie unter Token „**Internal**“ aus und tragen ggf. Ihr zuvor definiertes Passwort ein.

Abbildung 14



In das Feld „Zertifikatdaten“ kopieren Sie das Zertifikat „**Ihr ServerPass Zertifikat**“ - incl. der ---BEGIN... und ---END... Zeilen - aus Abbildung 10.

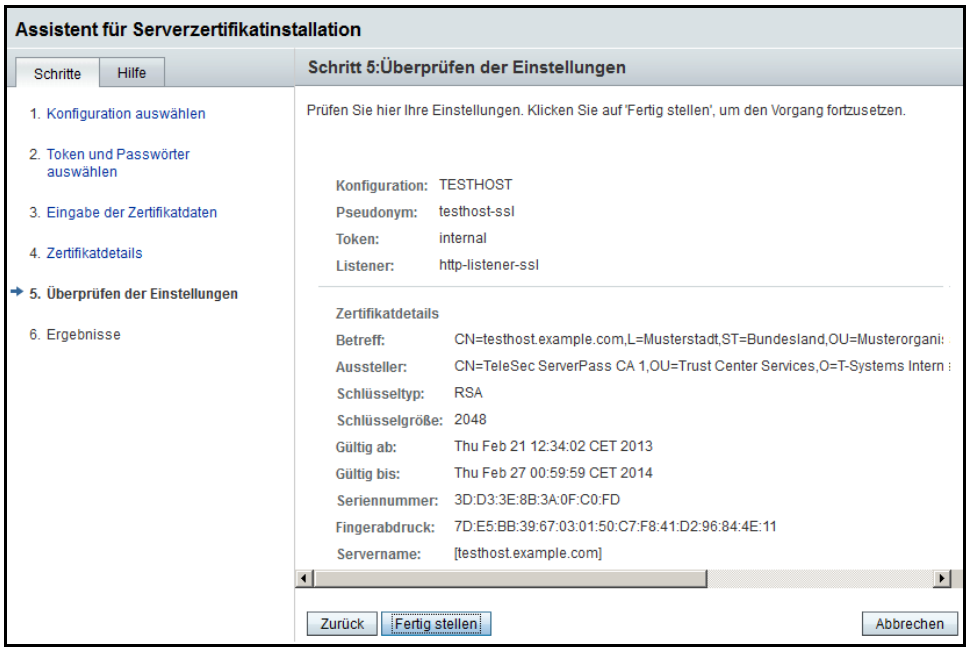
Abbildung 25



In Abbildung 25 merkt der Assistent an, dass bereits ein Zertifikat mit gleichlautenden Einträgen existiert wie im zu importierende Zertifikat. Das neue Zertifikat wird unter Verwendung des bestehenden Pseudonyms importiert.

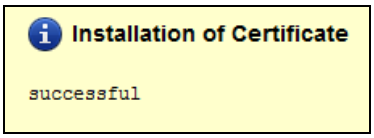
Auch muss das Zertifikat an den bestehenden HTTP-Listener gebunden, der für den SSL-Modus vorgesehen ist. Im Beispiel ist dies „http-listener-ssl“.

Abbildung 26



In Abbildung 26 werden die Details Ihres Serverzertifikats dargestellt.
Überprüfen Sie die Angaben und schließen den Import über „**Fertig stellen**“ ab.

Abbildung 27



Der erfolgreiche Import wird entsprechend quittiert.

Abschließend muss die Konfiguration noch „bereitgestellt“ werden.
Dies geschieht über den entsprechenden Button oben rechts - „**Bereitstellung steht aus**“, siehe Abbildung 38.

Abbildung 38

Nachdem die Bereitstellung durchgeführt wurde stellt sich die „Konfiguration Console“ wie folgt dar.

Abbildung 39

Der Import des erneuerten Zertifikats ist abgeschlossen.

2.5 Sicherung der Dateien

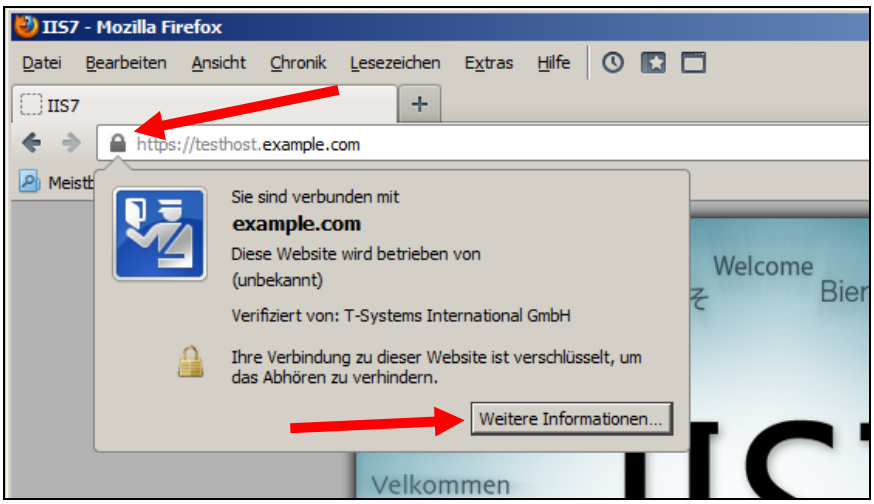
Es wird dringend empfohlen, die erzeugten Dateien zu sichern, z. B. auf einem externen Medium!
Gesichert werden sollten die Schlüssel-Dateien des virtuellen Hosts, „cert8.db“, „key3.db“. und „secmod.db“. In der Beispielkonfiguration befinden sie sich unter:
C:\Program Files\Oracle\WebServer7\https-TESTHOST\config\

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 40-42) sowie im Internet Explorer (Abbildung 43-45) aufgeführt.

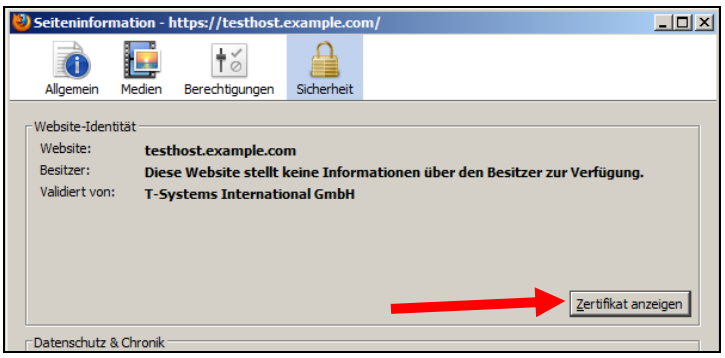
Firefox:

Abbildung 40 (Firefox 18):



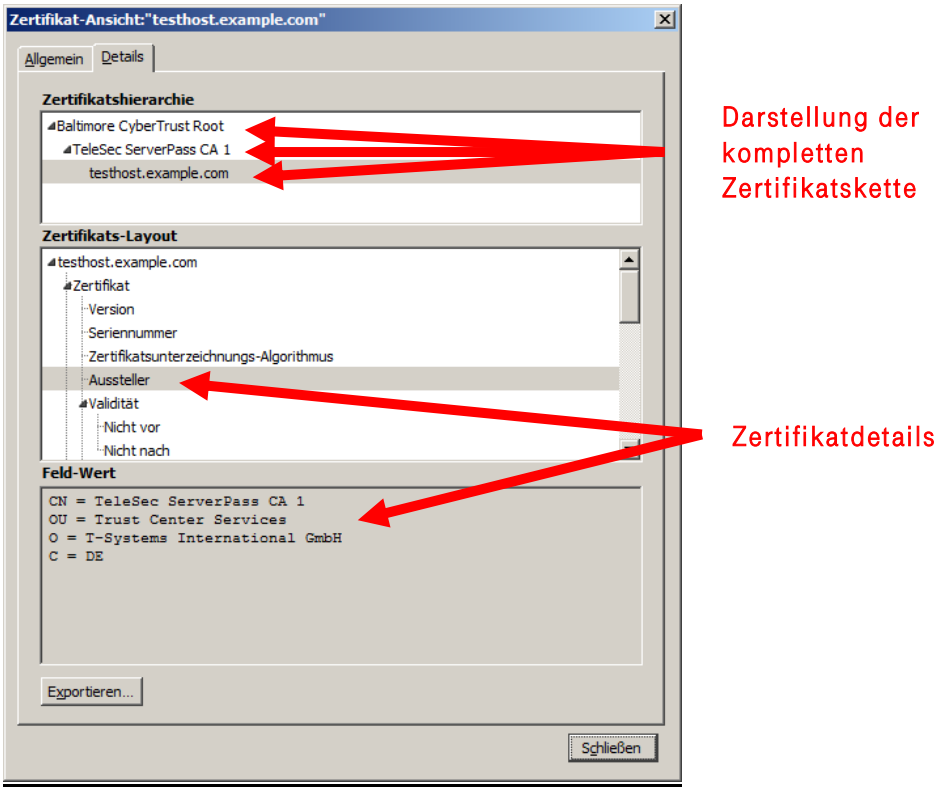
Beim Firefox lassen sich über einen Klick auf das Schloss Details zum verwendeten Zertifikat anzeigen.
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 41 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

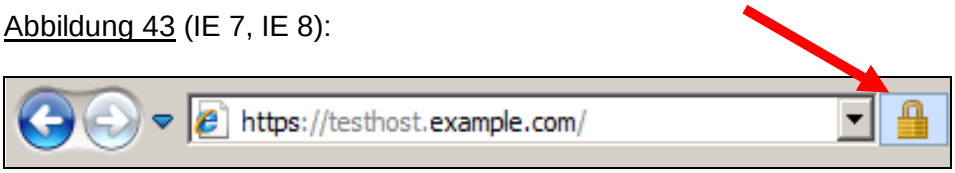
Abbildung 42 (Firefox 18):



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“

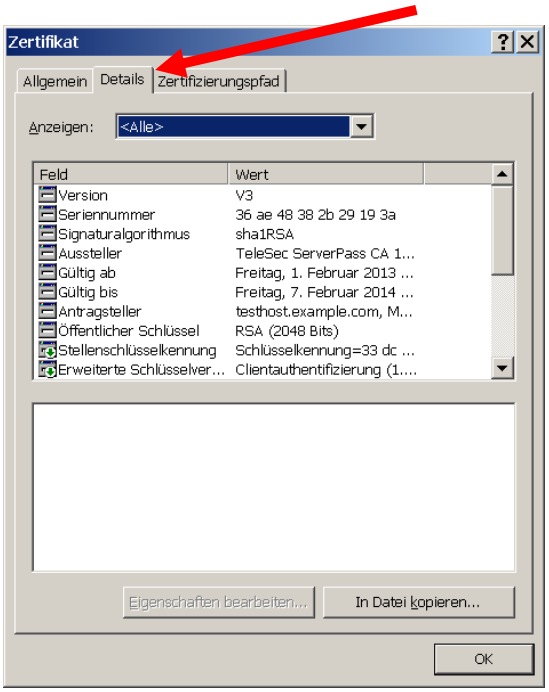
Internet Explorer

Abbildung 43 (IE 7, IE 8):



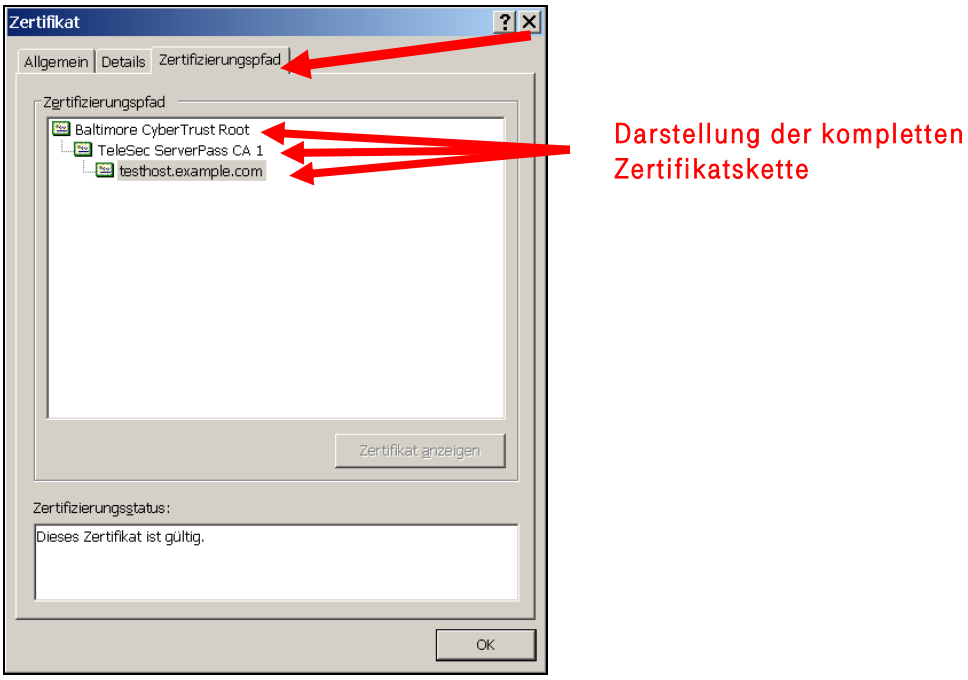
Beim Internet Explorer lassen sich die Zertifikatsdetails durch Doppelklick auf das Schloss anzeigen.
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung44.

Abbildung 44 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 54.

Abbildung 54 (Die Zertifikatskette)



So wie in Abbildung 54 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.