TeleSec ServerPass

Installation der CA-Zertifikate im MS IIS 7.0

Version: 1.2
Stand: 14.04.2014
Status: Final

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

Dateiname	Dokumentennummer	Dokumentenbezeichnung
serverpass_cainst_msiis_7_Final.doc		Installation des CA-Zertifikats MS iiS 6.0

Version	Stand	Status
1.2	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
Installation der CA-Zertifikate im MS IIS 7.0

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	15.12.2010	W. Bohn	Erster Entwurf
1.0	21.12.2010	W. Bohn	Inhalts- und Layoutanpassung
1.1	11.02.2013	W. Bohn	Inhaltliche Anpassung
1.2	10.02.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

1 Allgemeines

Dieses Dokument beschreibt die **Installation der CA-Zertifikate im Microsoft Internet-Information-Server, kurz IIS, Version 7.0**

Die Beschreibung bezieht sich auf folgende Softwarekonstellation:

Microsoft Internet Information Server 7.0, deutsch
Microsoft Server 2008 R2 Standard, deutsch
Browser: Internet Explorer ab Version 7 oder Firefox 18

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 Einbindung der CA-Zertifikate für den Einsatz im IIS 7.0. Die Einbindung beim IIS 7.5 verläuft ähnlich. Für die Einbindung der CA-Zertifikate im IIS 6.0 ist eine separate Anleitung verfügbar.
Bei korrekter Installation liefert der Webserver dem Client (z. B. Browser) neben dem Serverzertifikat auch die CA-Zertifikate des Ausstellers. Der Client kann die Prüfung des vollständigen Zertifizierungspfades vollziehen. Es erscheinen keine Warnhinweise.

Weiterführende Erklärungen über den Einsatz von SSL-Zertifikaten zur Authentifikation 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 bezgl. des erlaubten Zeichensatzes ab Kapitel 8.3.

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

Siehe hierzu: 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 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 auf unserer Internetseite herunterladen.

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

Hier werden ebenfalls alle relevanten Details wie Seriennummern, Laufzeiten, Finger-prints usw. der einzelnen Zertifikate angegeben.

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

2 Zertifikate herunterladen

Sie können die benötigten Zertifikate auf unterschiedlichem Wege herunterladen.

2.1 Download der Zertifikatskette aus „myServerPass“

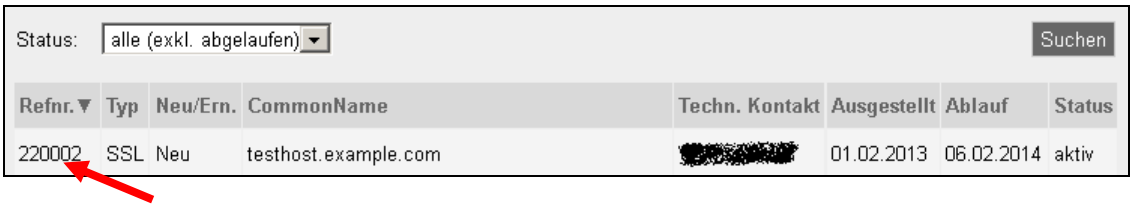
Sie erhalten das für Sie ausgestellte SSL-Server-Zertifikat und alle zugehörigen Zertifikate der ausstellenden Instanzen mit der Download-Datei Ihres Serverzertifikats. Verwenden Sie hierfür Ihr „myServerPass“ Konto.

Anmelden an „myServerPass“:
https://www.telesec.de/serverpass/ (→ myServerPass)

Wählen Sie den Menüpunkt „Meine Zertifikate“

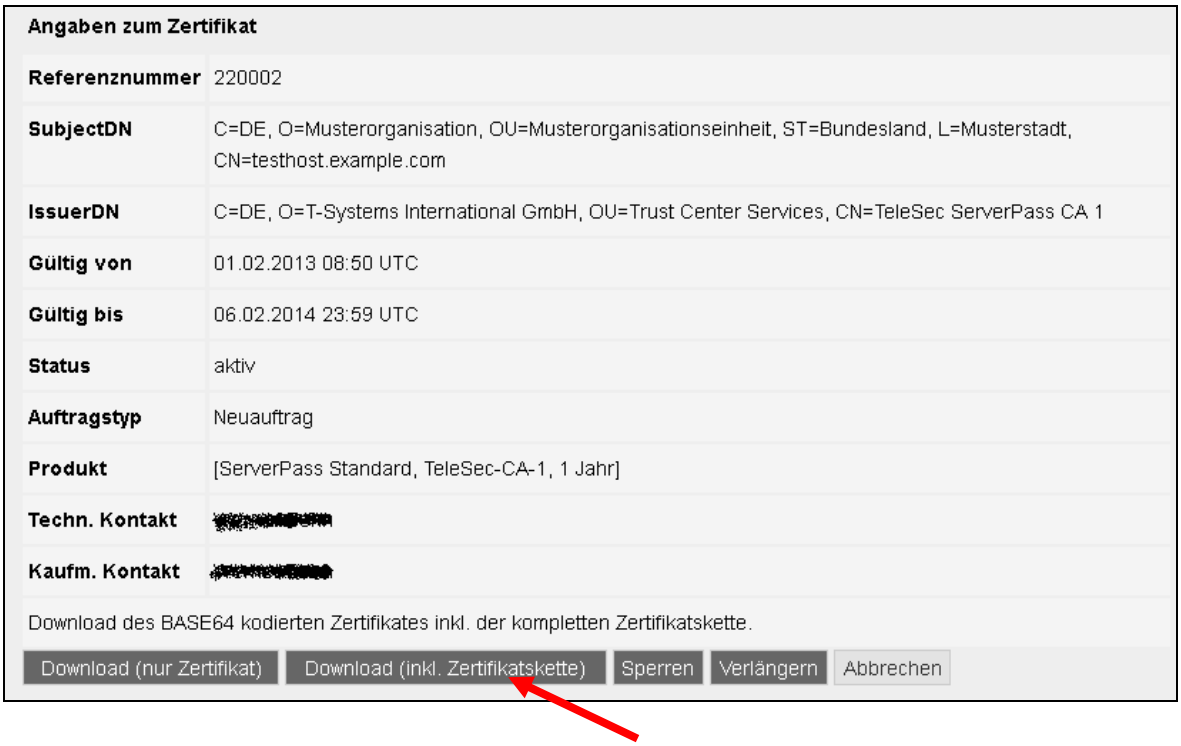
Hier werden nun alle Ihre Zertifikate aufgelistet.
Wählen Sie das herunter zuladende Zertifikat durch Klick auf die Referenznummer aus, siehe Abbildung 1.

Abbildung 1



Es werden zwei Download-Formate angeboten:
- Download (Nur Zertifikat)
- Download (inkl. Zertifikatskette)

Abbildung 2:



Wählen Sie das Format: „Download (inkl. Zertifikatskette)“, siehe Abbildung 2.

Anschließend 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 unter c:\.

So wie in Abbildung 3 dargestellt, enthält die herunter geladene Datei mehrere Zertifikate. Im Einzelnen sind dies:

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

Abbildung 3 (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-----
MIIGyzCCBbOgAwIBAgIIUIRr2EVSs6UwDQ
…
4AQiYmLrtMxr6HPGNIIr
-----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-----
```

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 zunächst das CA-Zertifikat „TeleSec ServerPass CA 1“ inkl. der „---BEGIN... und ---END... “ Zeilen (hier magenta markiert) und speichern es als Textdokument in einer eigenen Datei ab, zum Beispiel „TeleSec_ServerPass_CA_1.cer“. Bitte verwenden Sie hierbei die Endung „.cer" oder „.crt“.
- Der Import des Root-Zertifikats (hier grün markiert) ist in der Regel nicht erforderlich. Wird es dennoch benötigt, so markieren Sie das Root-Zertifikat „Baltimore CyberTrust Root“ inkl. der „---BEGIN... und ---END...“ Zeilen (hier grün

markiert) und speichern es als Textdokument in einer eigenen Datei ab, zum Beispiel „BaltimoreCyberrustRoot.cer“. Bitte verwenden Sie hierbei die Endung „.cer" oder „.crt“.

2.2 Direkter Download von CA- und Root-Zertifikat

Alternativ kann man CA- und Root-Zertifikat separat herunterladen.

https://www.telesec.de/serverpass/

(→ Support → Root- / Sub-CA-Zertifikate)

2.2.1 Download des Zertifikats „TeleSec ServerPass CA 1

Unter „CA-Zertifikate“ wählen Sie diesen Eintrag aus: „TeleSec ServerPass CA 1“ .
Es wird der Download eine ZIP-Files angeboten, siehe Abbildung 4. Es beinhaltet das Zertifikat in den Formaten DER und BASE64..

Abbildung 4:

Wählen Sie den Link um das Zertifikat zu laden.

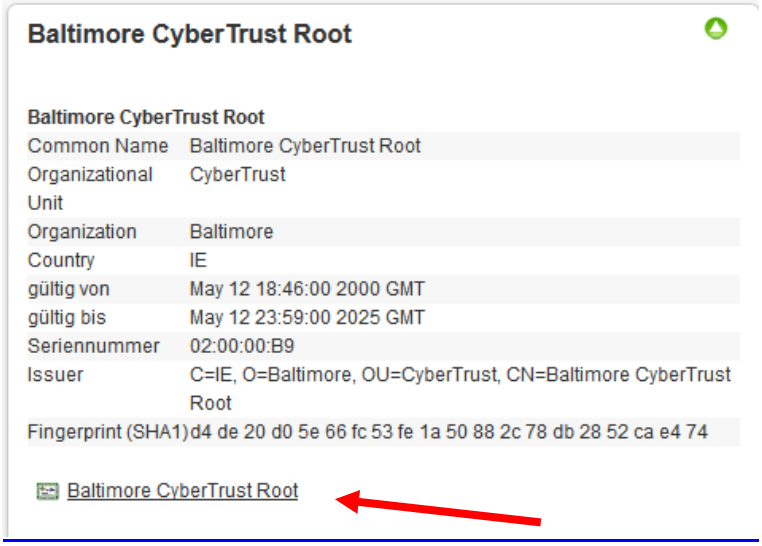
Abbildung 5:

Markieren Sie die Option „Speichern“ und legen einen Speicherort fest, siehe Abbildung 5.

2.2.2 Download des Zertifikats „Baltimore CyperTrust Root“:

Unter „Root-Zertifikate wählen diesen Eintrag aus: „Baltimore CyberTrust Root“ .
Es werden zwei Downloadformate angeboten, siehe Abbildung 6.

Abbildung 6:



Wählen Sie den Link um das Zertifikat zu laden.

Abbildung 7:

Markieren Sie die Option Speichern“ und legen einen Speicherort fest, siehe Abbildung 7.

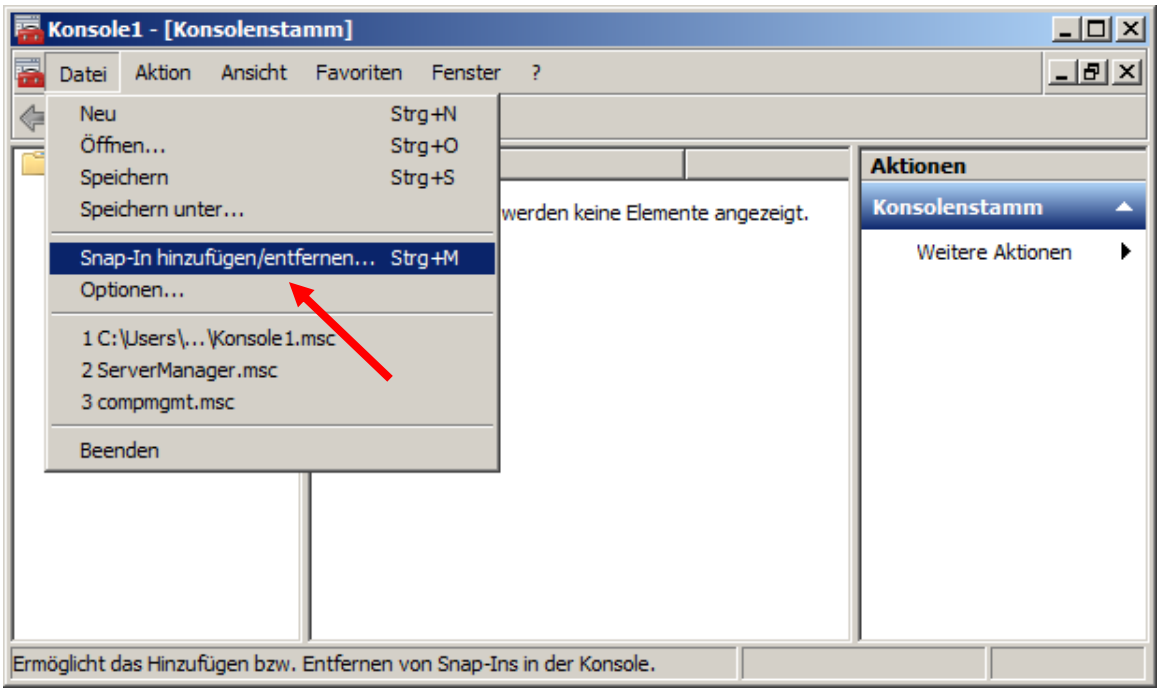
3 Importieren der Zertifikate

Ihnen sollten nun folgende Zertifikate zur Verfügung stehen:

Das Zertifikat „TeleSec ServerPass CA1“ und ggf. auch das Zertifikat „Baltimore CyberTrust Root“.

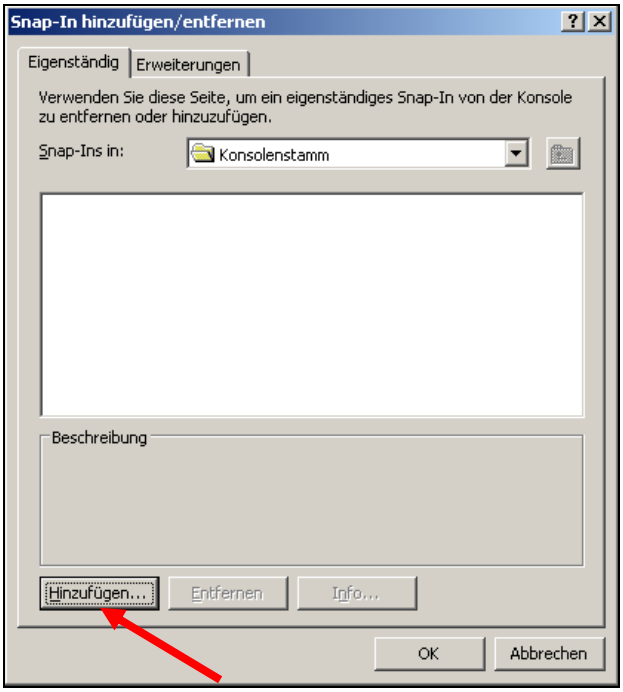
Für den Import des CA-Zertifikats wird hier der Weg über die „Management-Konsole“, kurz „mmc“ aufgezeigt.
Start der Management-Konsole: **Start** → **Ausführen** → **mmc**
Es öffnet sich die Management-Konsole, siehe Abbildung 8.

Abbildung 8 (Die MMC-Konsole)



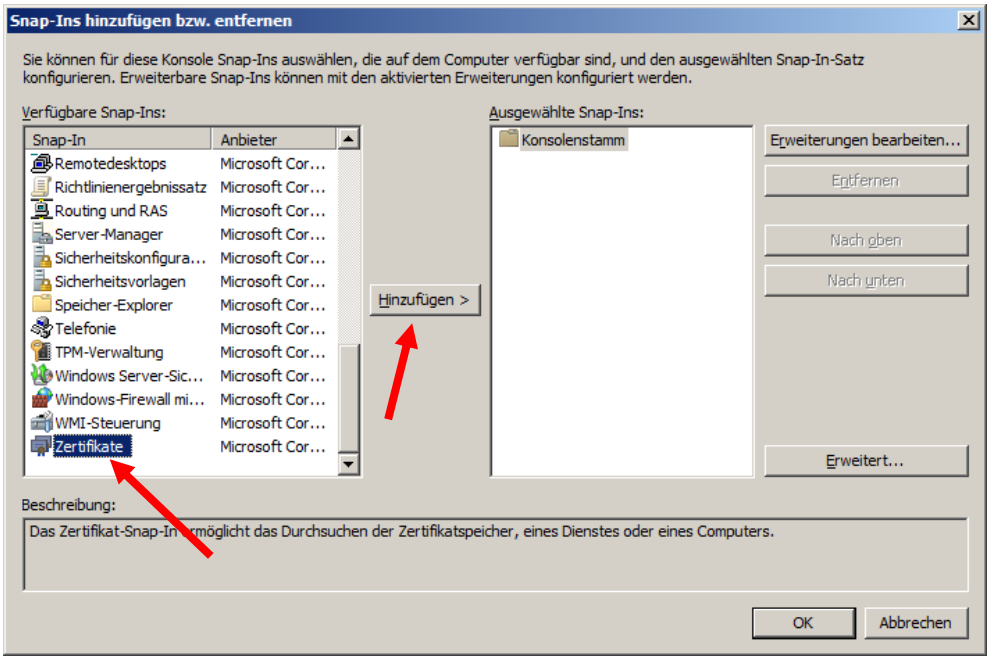
Zunächst muss das „Snap-IN“ für die Zertifikatsverwaltung hinzugefügt werden:
Klicken auf „**Datei**“ → „**Snap-In hinzufügen/entfernen**“, es öffnet sich Abbildung 9.

Abbildung 9 (Liste der Snap-Ins)



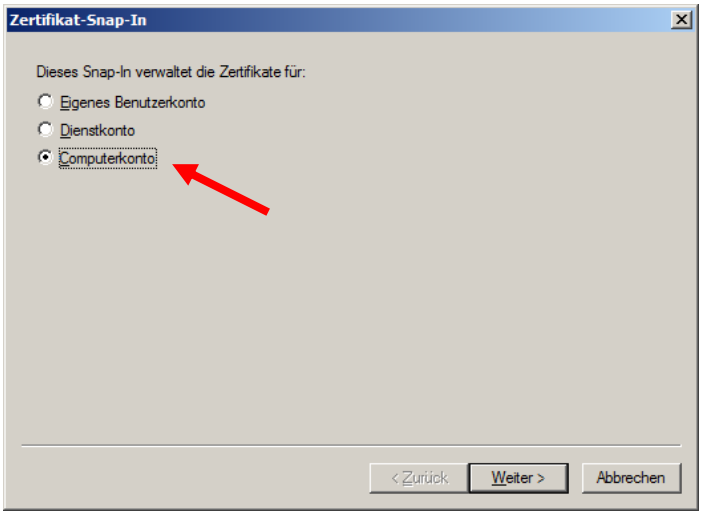
Über den Button „**Hinzufügen**“ erreicht man die verfügbaren „Snap-Ins“.

Abbildung 10



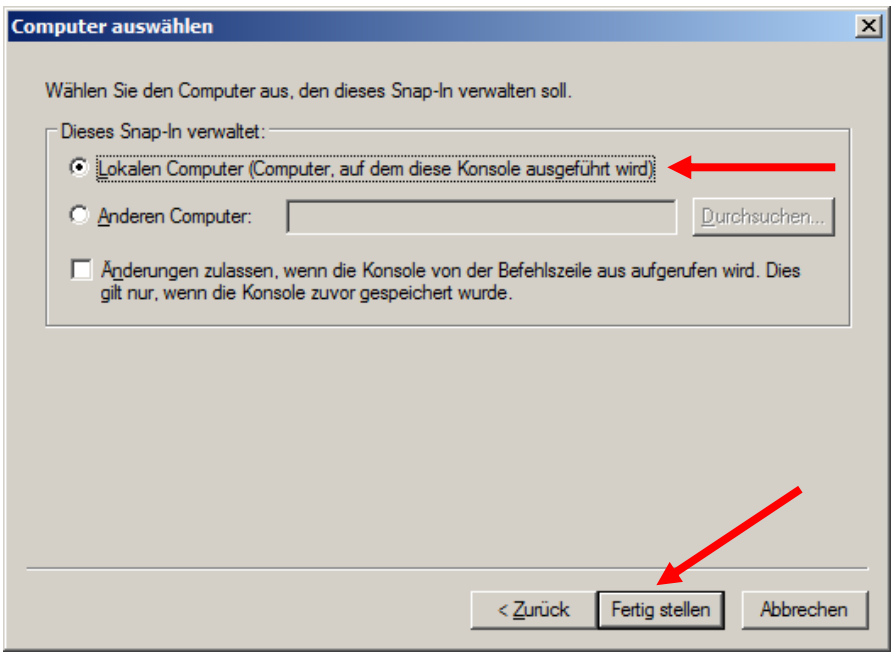
Wie in Abbildung 10 dargestellt, erfolgt die Auswahl des Snap-Ins „**Zertifikate**“. Klicken auf „**Hinzufügen**“.

Abbildung 11



In Abbildung 11 erfolgt die Auswahl des Eintrages „**Computerkonto**“.

Abbildung 12

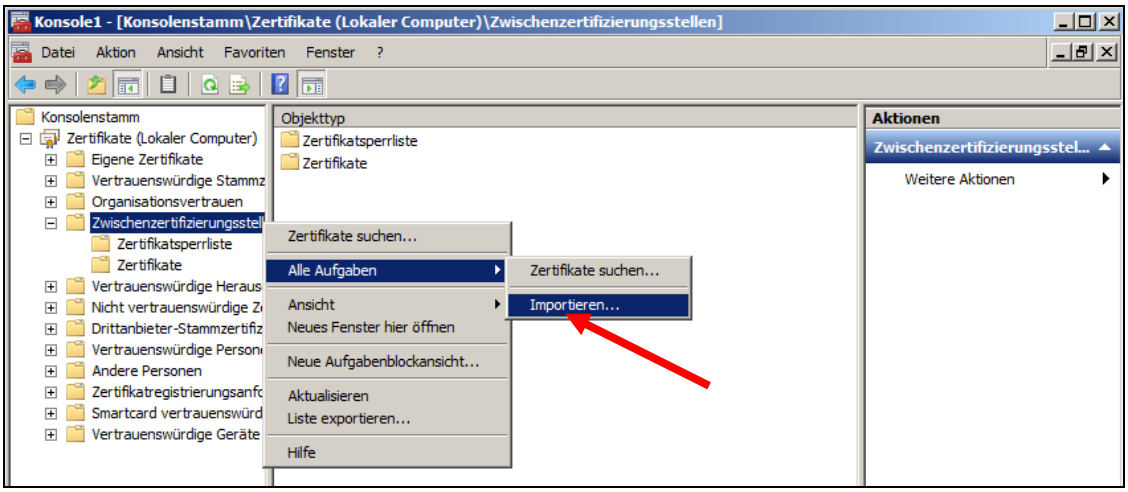


Hier erfolgt die Auswahl des Eintrages „**Lokaler Computer**“ als zu verwaltender Computer.
Anschließend klicken auf „**Fertig stellen**“. Das darauf folgende Fenster wird einfach mit Klick auf „**OK**“ bestätigt.

3.1 Import des CA-Zertifikats:

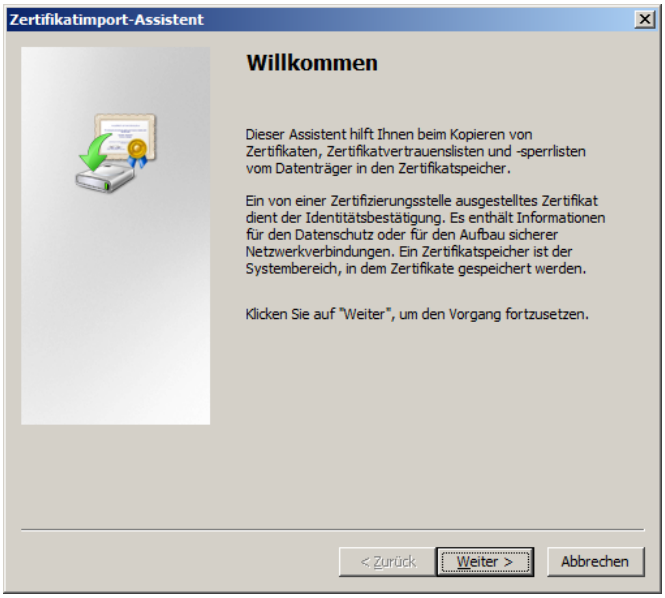
Nachdem das „Snap-In“ für die Zertifikatsverwaltung hinzugefügt wurde, erfolgt der eigentliche Import des CA-Zertifikats.

Abbildung 13



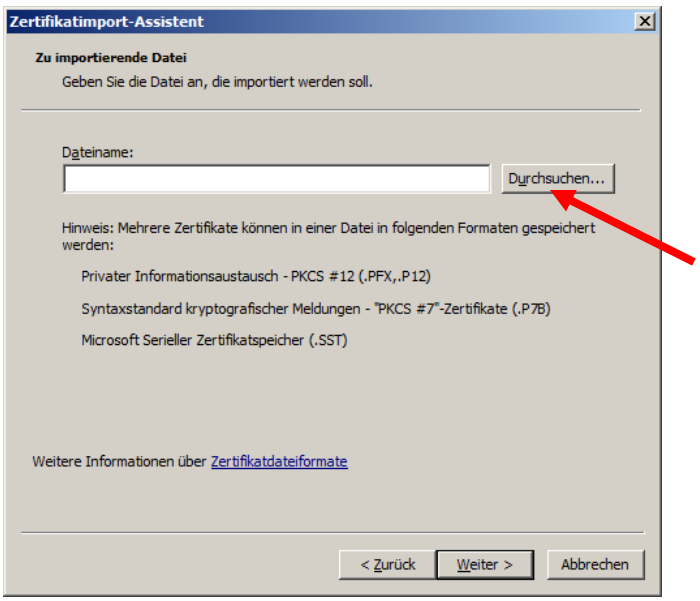
In der Konsole öffnen Sie den Zertifikatsbaum unter dem Eintrag „**Zertifikate (Lokaler Computer)**. Nun den Zweig für die „**Zwischenzertifizierungsstellen**“ und anschließend den Eintrag „**Zertifikate**“ mit der rechten Maustaste markieren und den Menüeintrag „**Alle Aufgaben**“ und dann „**Importieren**“ auswählen.

Abbildung 14 (Der Zertifikatimport-Assistent):



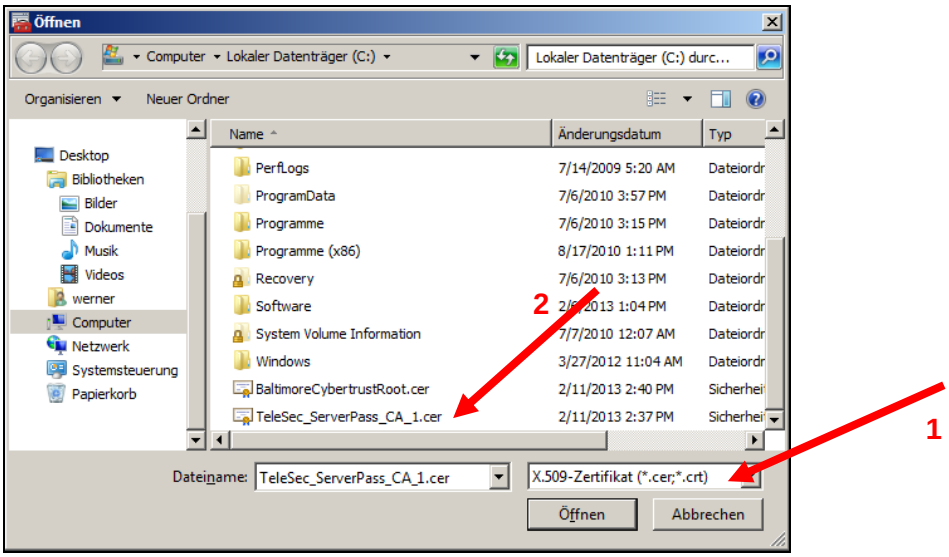
Dieses Fenster bestätigen Sie mit „**Weiter**“.

Abbildung 15



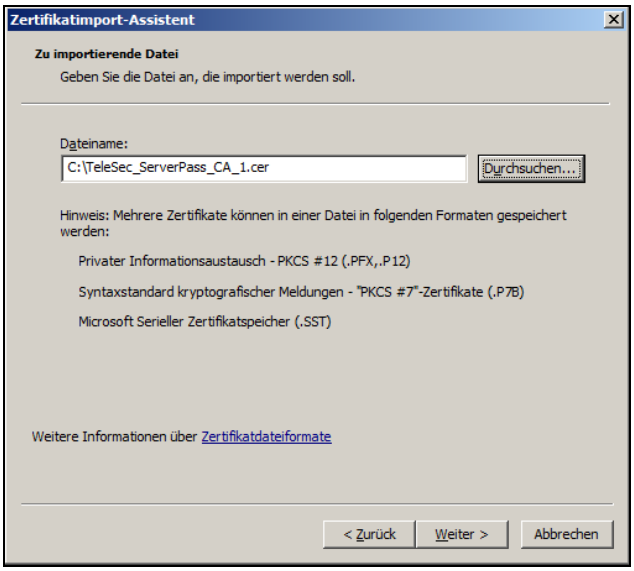
In Abbildung 15 legen Sie über den Button „**Durchsuchen**“ den Pfad zur Importdatei fest.

Abbildung 16



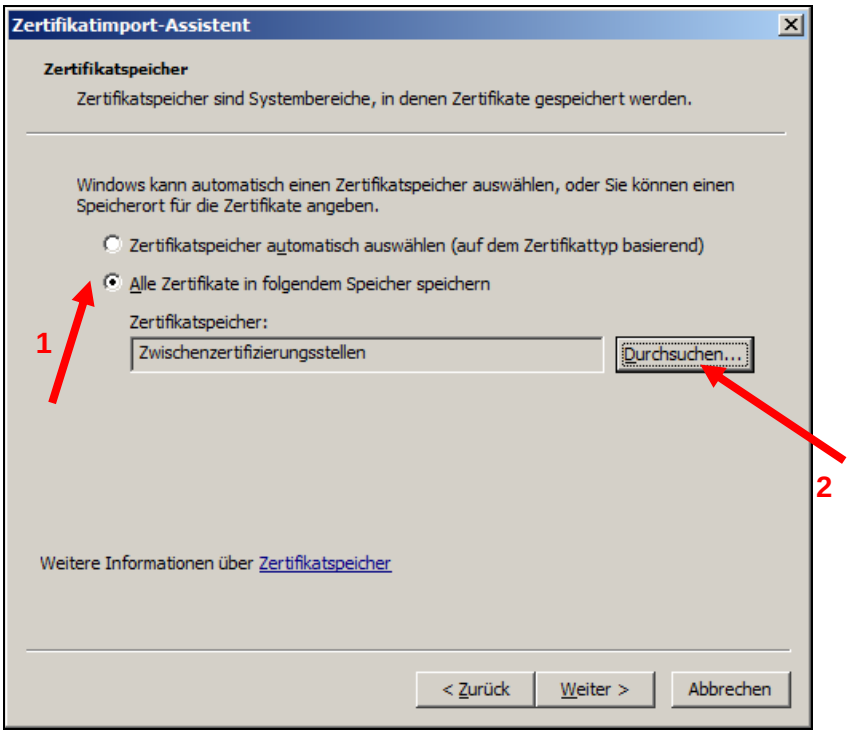
Legen Sie die Importdatei fest. ggf. muss der Datei eingestellt werden auf „X.509-Zertifikat, z. B. „c:\ TeleSec_ServerPass_CA_1.cer“, siehe Abbildung 16.
Nachdem die Importdatei feststeht klicken Sie auf „**Öffnen**“, es erscheint Abbildung 17.

Abbildung 17



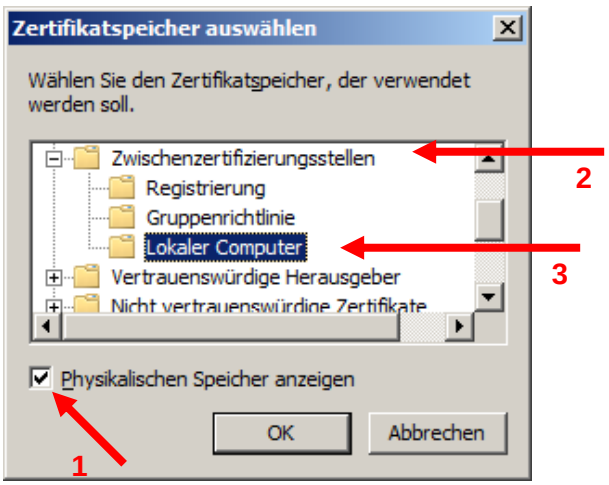
In Abbildung 17 klicken Sie einfach auf „**Weiter**“.

Abbildung 18



Wie in Abbildung 18 dargestellt, wird zunächst der Eintrag „**Alle Zertifikate in folgendem Speicher speichern**“ aktiviert und anschließend durch Drücken auf „**Durchsuchen**“ der auszuwählende Zertifikatsspeicher aufgelistet.

Abbildung 19 (Auswahl des Zertifikatsspeichers)

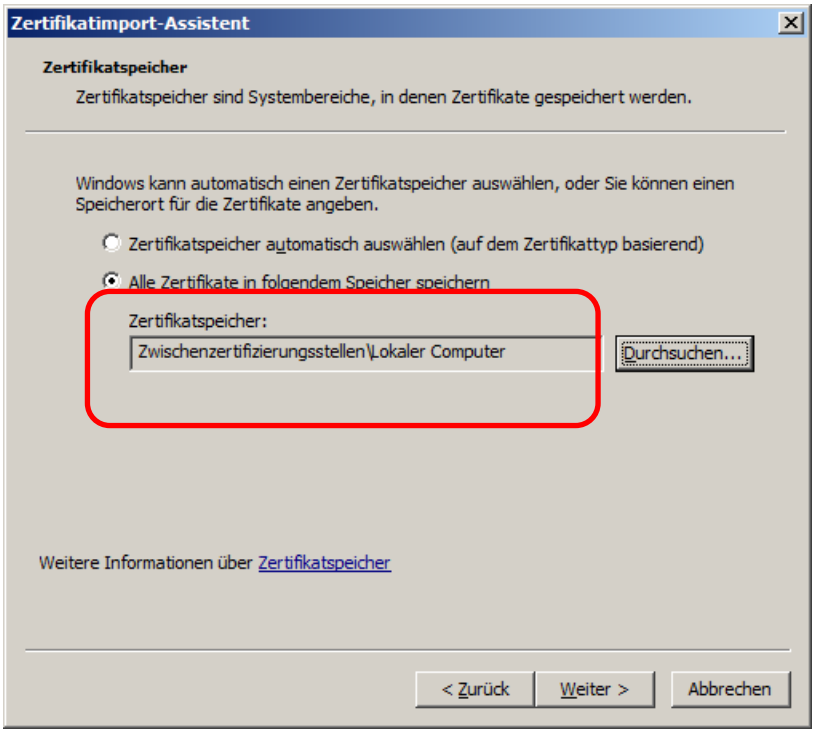


Nun folgt die Auswahl des Zertifikatspeichers.

Die Festlegung des korrekten Zertifikatsspeicher ist extrem wichtig!
Wird hier nicht der korrekte Zertifikatsspeicher ausgewählt, kann der Webserver nicht auf das importierte CA-Zertifikat zugreifen.

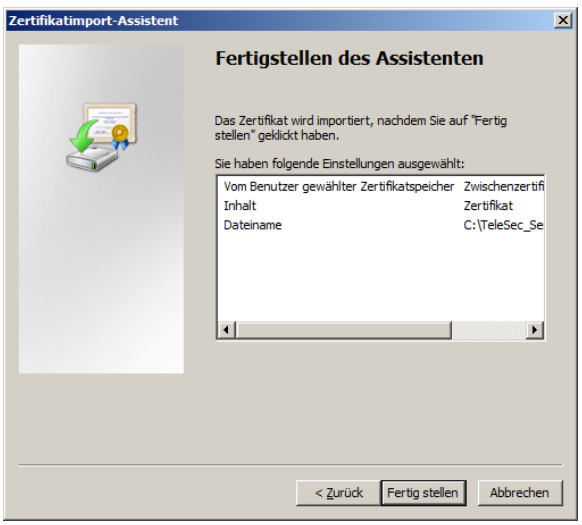
Zunächst wird das Häkchen zur Ansicht des „**Physikalischen Speichers**“ markiert. Anschließend wird der Zweig für „**Zwischenzertifizierungsstellen**“ erweitert. Abschließend markiert man den darunter liegende Eintrag „**Zertifikate**“ und bestätigt die Eingabe durch „**OK**“.

Abbildung 20, (Anzeige des korrekten Zertifikatsspeichers):



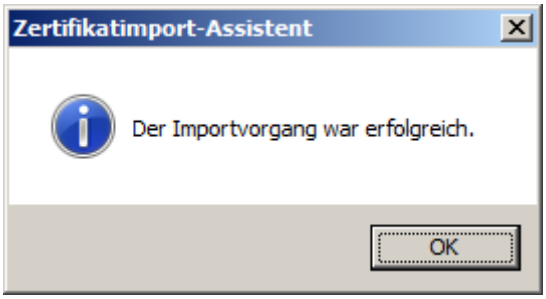
Der Zertifikatsspeicher sollte nun eingestellt sein auf:
„**Zwischenzertifizierungsstellen\Lokaler Computer**“, siehe Abbildung 20.
Klicken auf „**Weiter**“.

Abbildung 21



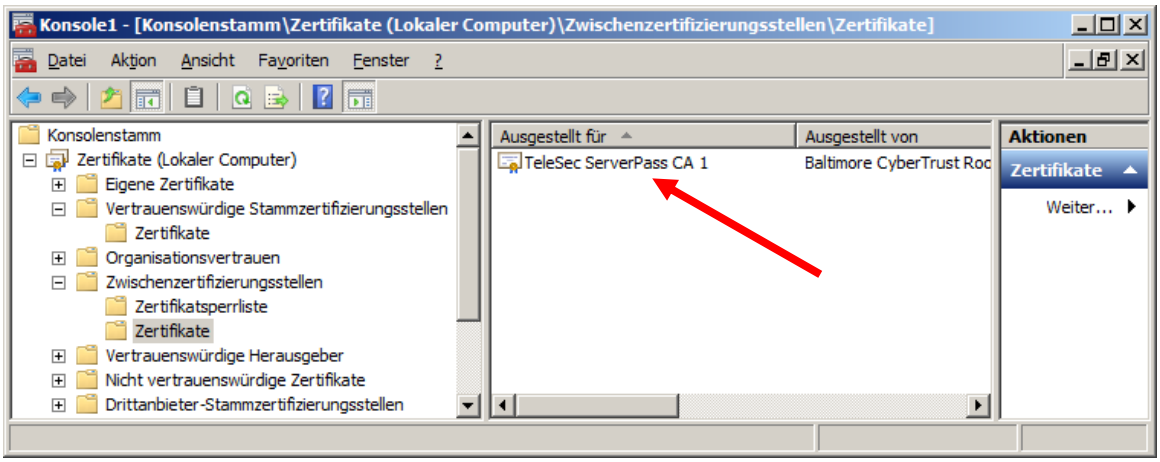
In Abbildung 22 werden die Details zum Zertifikatsimport aufgelistet. Klicken auf „**Fertig stellen**“ schließt den Import ab.

Abbildung 23



Der erfolgreiche Import wird bestätigt, wie in Abbildung 23 angegeben.

Abbildung 24



Wie in Abbildung 24 dargestellt, muss nun das zuvor importierte Zertifikat unter „Zwischenzertifizierungsstellen → „Zertifikate“ erscheinen, evtl. muss die Anzeige aktualisiert werden (drücken der Taste „F5“). ggf. werden hier auch weitere Zertifikate aufgelistet.

Anschließend wird die Konsole gespeichert, z. B. unter „…/Verwaltung/Konsole1.msc“. Soll auch das Root-Zertifikat importiert werden, so lassen Sie Konsole geöffnet und fahren fort mit Punkt 3.2, ansonsten kann die Konsole nun geschlossen werden.

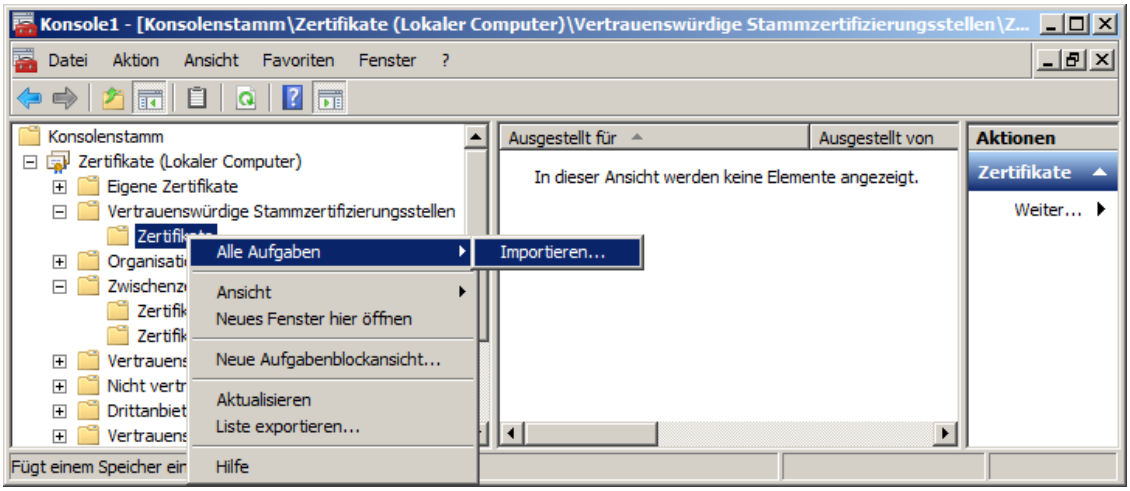
3.2 Falls erforderlich, Import des Root-Zertifikats

Sollte das Root-Zertifikat auf dem Serversystem noch nicht bekannt sein, so empfiehlt sich der Import des Root-Zertifikats.

Ob das Root-Zertifikat bereits installiert wurde, kann z. B. über die „Management-Konsole“, kurz „mmc“ geprüft werden.

Start der Management-Konsole: **Start** → **Ausführen** → **mmc**
Es öffnet sich die Management-Konsole. Über den Menüpunkt „**Datei**“ → „**Öffnen**“ wählen Sie die zuvor abgespeicherte Konsolen-Datei, z. B. „…/Verwaltung/Konsole1.msc“, es erscheint Abbildung 25.

Abbildung 25



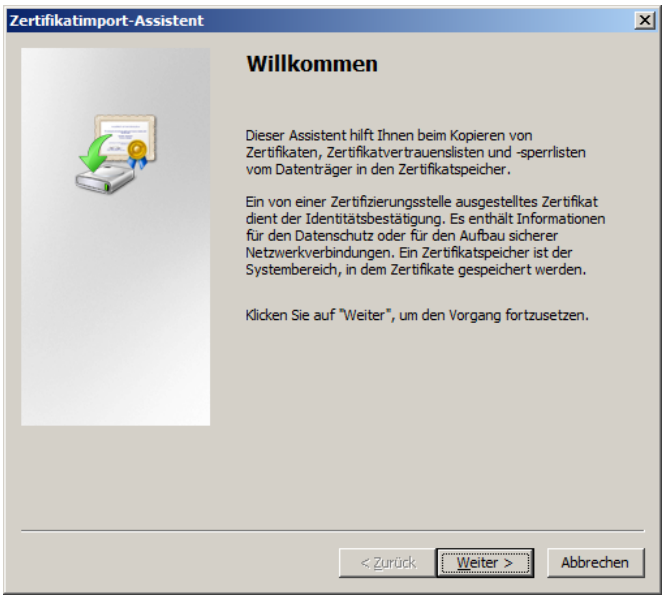
Aktuell wir im Zertifikatsspeicher der „Vertrauenswürdigen Stammzertifizierungsstellen“ das erforderliche Root-Zertifikat noch nicht angezeigt.

Nun kann der Importvorgang gestartet werden, siehe Abbildung 25.

Markieren Sie den Eintrag unter:

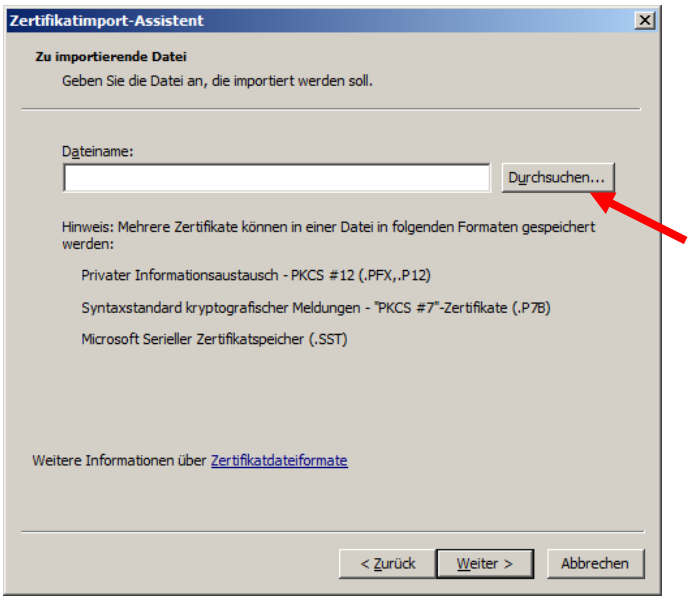
„**Konsolenstamm**“ → „**Zertifikate**“ → „**Vertrauenswürdige Stammzertifizierungsstellen**“ → „**Zertifikate**“ mit der rechten Maustaste und wählen „**Alle Aufgaben**“ → „**Importieren**“, es erscheint Abbildung 26

Abbildung 26



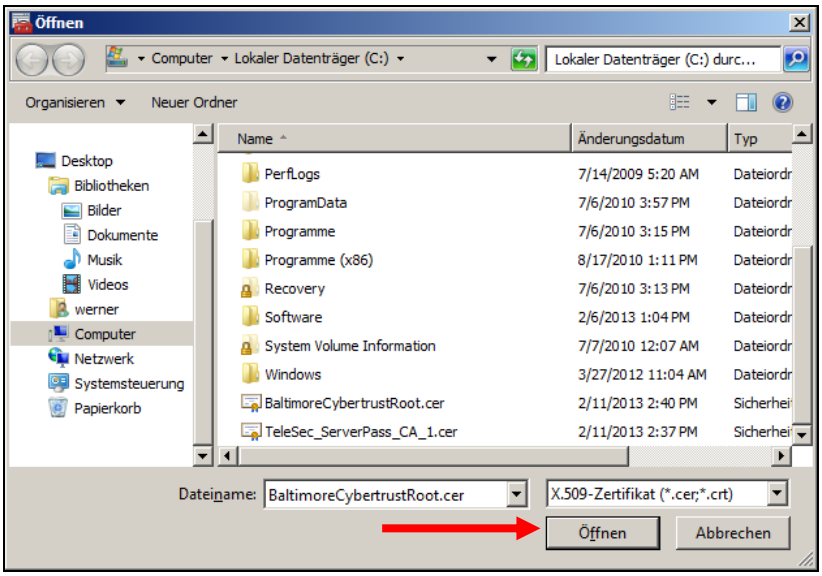
Es öffnet sich das Begrüßungsfenster des Zertifikat-Importassistenten. Dieses Fenster bestätigen Sie mit „**Weiter**“.

Abbildung 27



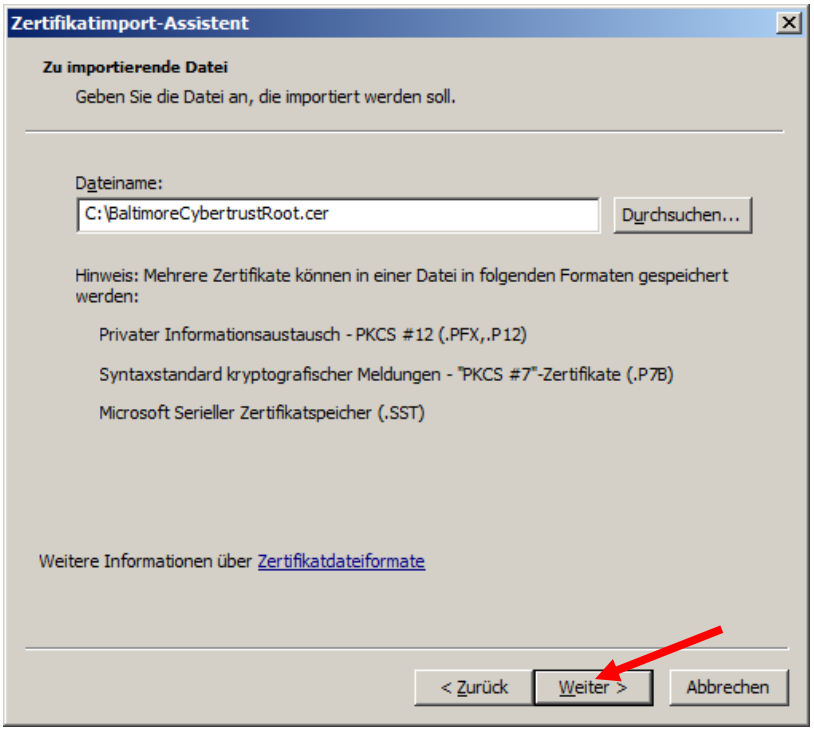
Über den Button „**Durchsuchen**“ wählen Sie nun den Pfad zur Importdatei des Root-Zertifikats aus.

Abbildung 28



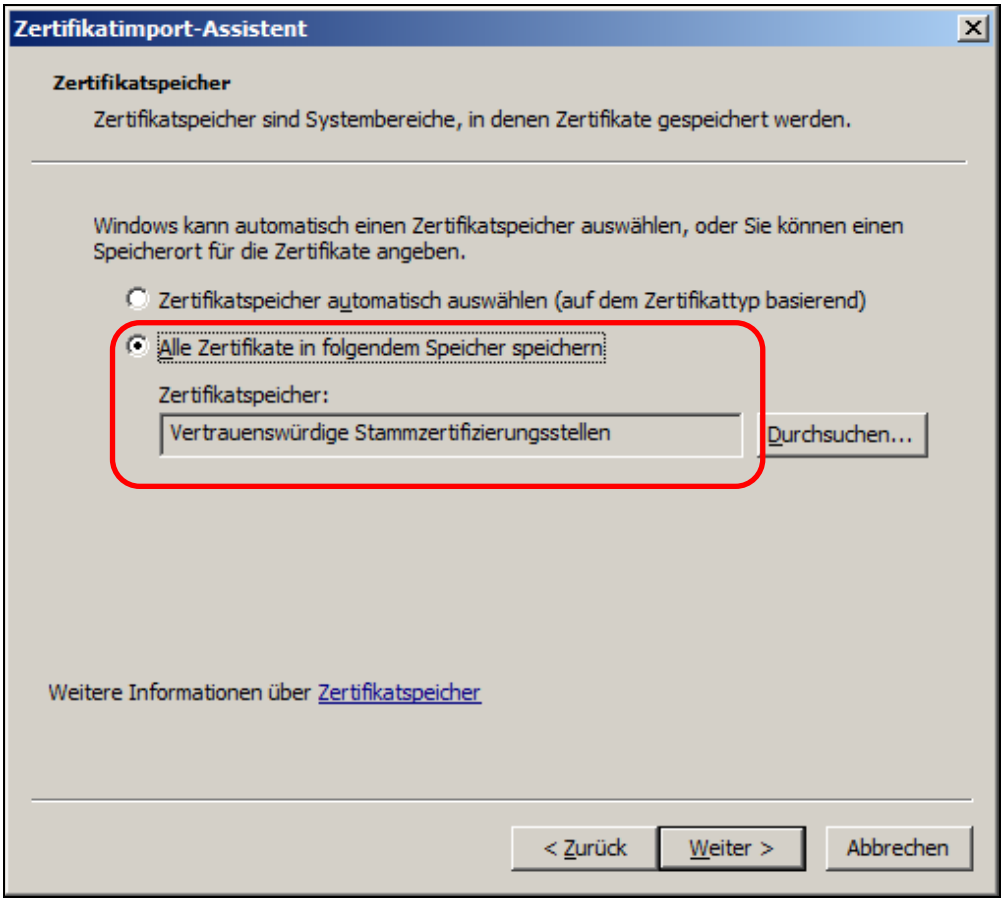
Legen Sie die Importdatei fest. Ggf. muss der Datei eingestellt werden auf „X.509-Zertifikat, z. B. „c:\ BaltimoreCyberTrustRoot.cer“, siehe Abbildung 265.
Nachdem die Importdatei feststeht klicken Sie auf „**Öffnen**“, es erscheint Abbildung 29.

Abbildung 29



Nachdem die Importdatei ausgewählt wurde, klicken Sie auf „**Weiter**“.

Abbildung 30



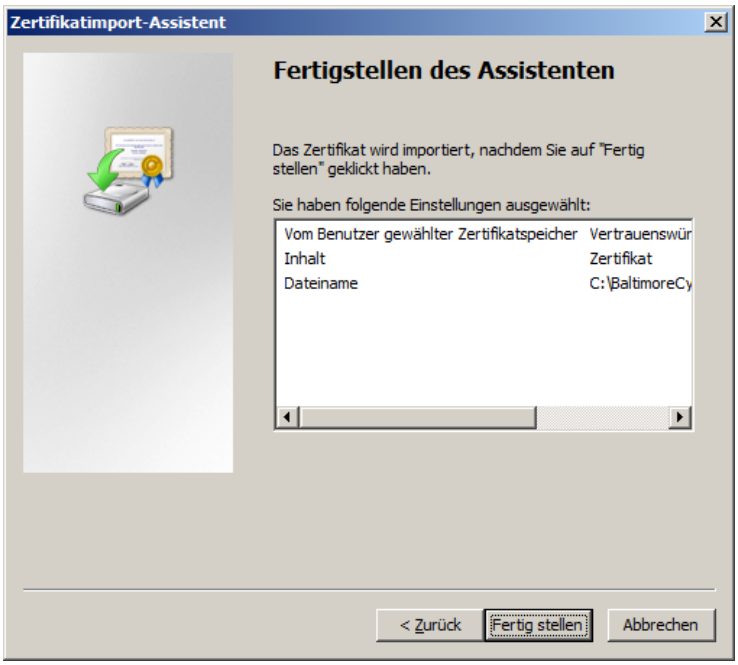
Die Festlegung des korrekten Zertifikatsspeichers ist extrem wichtig!
Wird hier nicht der korrekte Zertifikatsspeicher ausgewählt, kann der Webserver nicht auf das importierte Root-Zertifikat zugreifen.

Wie in Abbildung 30 dargestellt, muss der Zertifikatsspeicher eingestellt werden auf: „**Vertrauenswürdige Stammzertifizierungsstellen**“.

Falls nicht, stellen Sie ihn ein über die Option „**Durchsuchen**“.

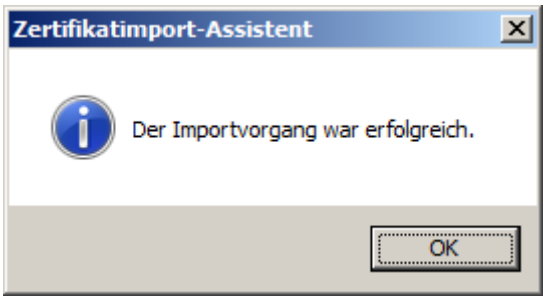
Anschließend klicken auf „**Weiter**“.

Abbildung 31



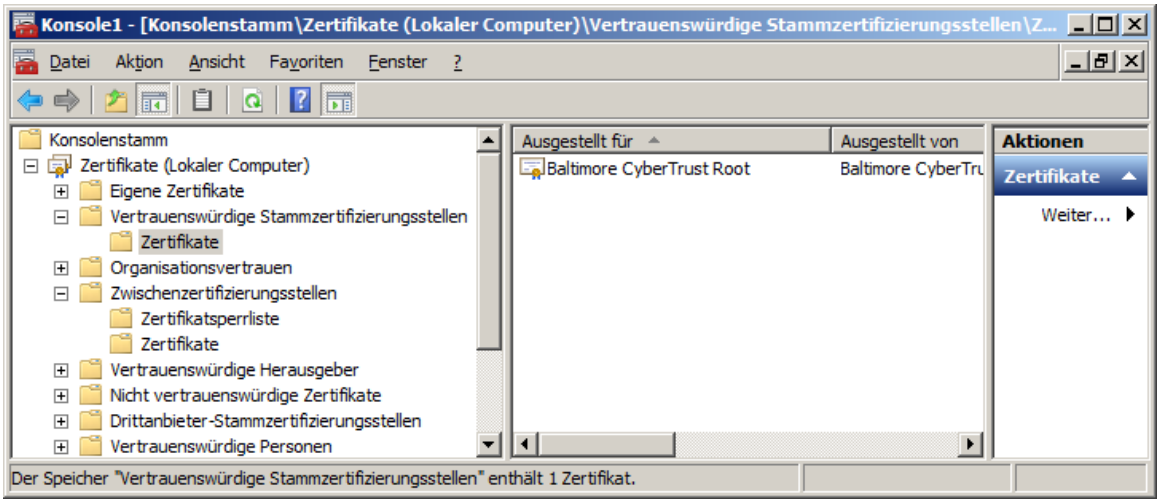
In Abbildung 31 werden die Details zum Zertifikatsimport aufgelistet. Klicken auf „**Fertig stellen**“ schließt den Import ab.

Abbildung 32



Der erfolgreiche Import wird bestätigt, wie in Abbildung 32 angegeben.

Abbildung 33



Wie in Abbildung 33 dargestellt, muss nun das zuvor importierte Zertifikat unter „Zwischenzertifizierungsstellen → „Zertifikate“ erscheinen, evtl. muss die Anzeige aktualisiert werden (drücken der Taste „F5“). ggf. werden hier auch weitere Zertifikate aufgelistet.

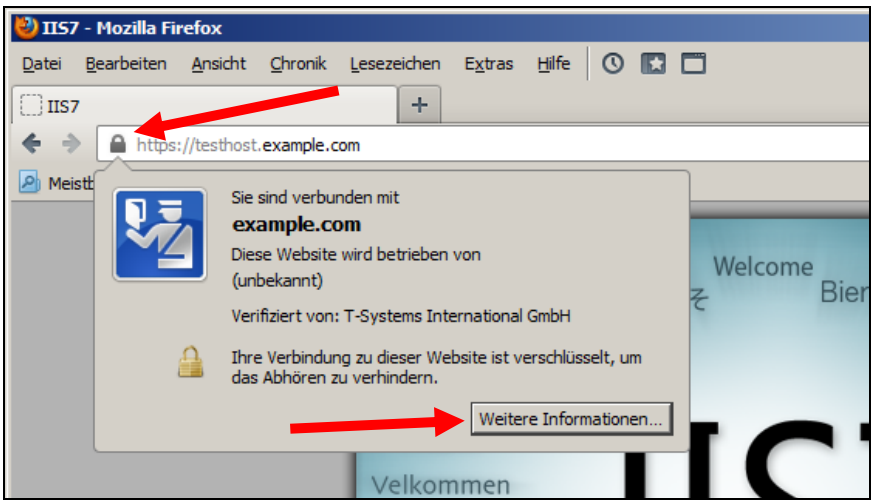
Anschließend wird die Konsole gespeichert, z. B. unter „…/Verwaltung/Konsole1.msc“. Der Import ist abgeschlossen und die Konsole nun geschlossen werden.

4 Kontrolle der Installation

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 34-36) sowie im Internet Explorer (Abbildung 37-39) aufgeführt.

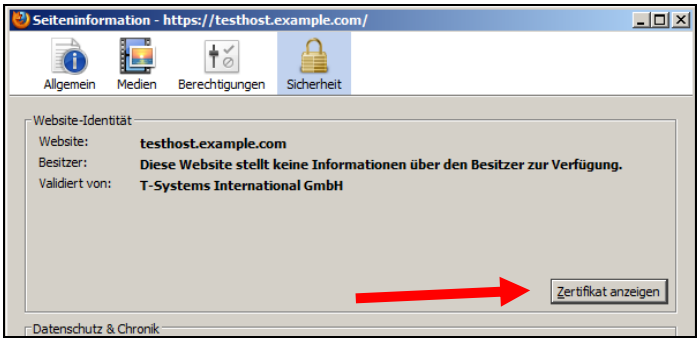
Firefox:

Abbildung 34 (Firefox 18):



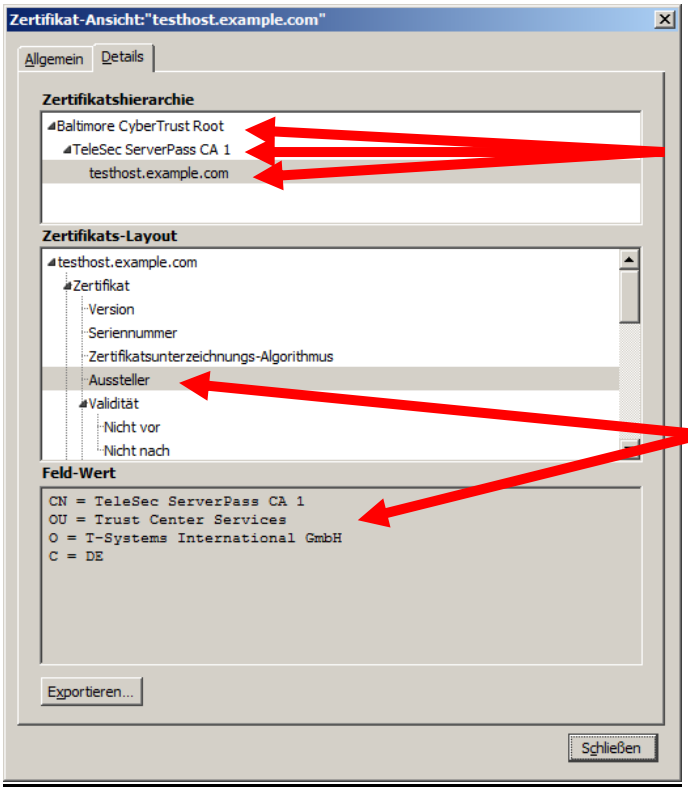
Beim Firefox lassen sich über einen Klick auf das Schloss Details zum verwendeten Zertifikat anzeigen.
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 35 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

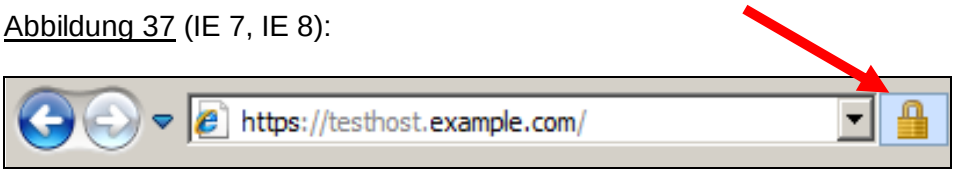
Abbildung 36 (Firefox 18):



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“

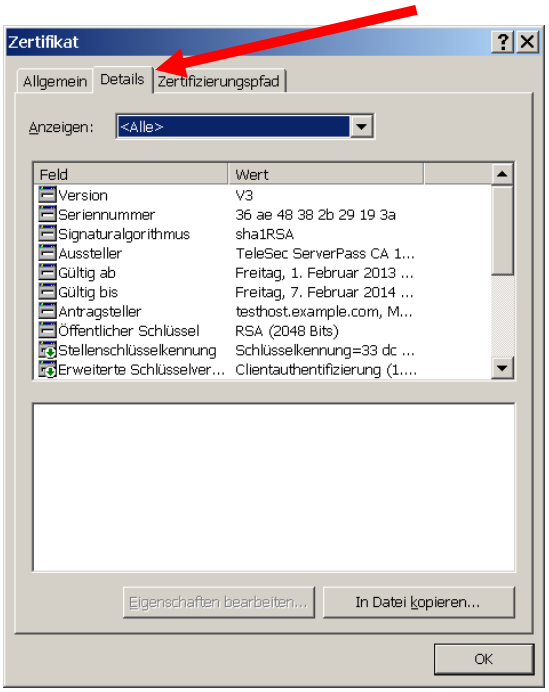
Internet Explorer

Abbildung 37 (IE 7, IE 8):



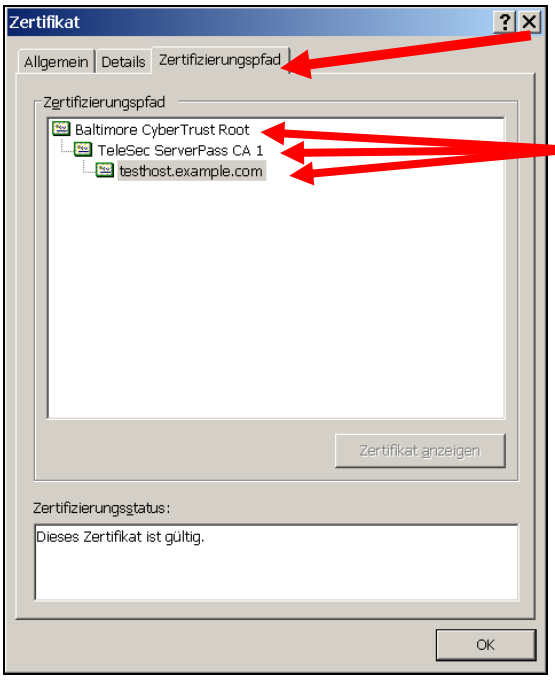
Beim Internet Explorer lassen sich die Zertifikatsdetails durch Doppelklick auf das Schloss anzeigen.
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 38.

Abbildung 38 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 39.

Abbildung 39 (Die Zertifikatskette)



Darstellung der kompletten

So wie in Abbildung 39 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.

5 Verwendung von Testzertifikaten

Über das Webportal „myServerPass“ ist die Beauftragung von kostenlosen Testzertifikaten möglich.

TeleSec ServerPass Test hat eine Gültigkeit von 30 Tagen und wird nicht unterhalb einer international etablierten Root ausgestellt.

Clients (Browser), die einen mit einem Test-Server-Zertifikat ausgestatteten Webserver kontaktieren, erhalten einen entsprechenden Warnhinweis.

Sollen Test-CA- und Test-Root-Zertifikat im Webserver installiert werden, so entspricht die Vorgehensweise im Wesentlichen dem zuvor gezeigten Ablauf. Lediglich die Bezeichnung der Zertifikate weicht ab.

Jedoch sind die „Ausstellenden Instanzen“ lediglich über das Webportal „myServerPass“ verfügbar.

Analog zum gezeigten Ablauf laden Sie Ihr Testzertifikat incl. Zertifikatskette im Webportal

„myServerPass“ herunter. Die herunter geladene Datei enthält ebenfalls drei Zertifikate, die Bezeichnung weicht jedoch wie folgt ab:

1. Das eigentliche „Test Serverzertifikat“, auch User-Zertifikat genannt.
2. Das Zertifikat „Deutsche Telekom Test CA 1“, auch CA-Zertifikat genannt.
3. Das Test- Root-Zertifikat „Deutsche Telekom Test Root CA 1“, auch Root-Zertifikat genannt.

Zur Installation folgen Sie dieser Anleitung von Beginn an.

Zusätzlich kann das Test-Root-Zertifikat im Browserclient importiert werden.

Dies geschieht zumeist über die Zertifikatsverwaltung des Webbrowser. Der Ablauf kann i. d. R. den Hilfe- sowie Support-Seiten der einzelnen Hersteller entnommen werden