TeleSec ServerPass

Zertifikats-Requesterzeugung mit dem MS IIS 7.0

Version: 2.6
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_msiis_7.doc		Requesterzeugung Microsoft IIS 7.0 Webserver

Version	Stand	Status
2.6	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-Requesterzeugung mit dem MS IIS 7.0

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	15.11.2008	W. Bohn	Entwurf
0.2	15.12.2008	M. Graf, L. Eickholt	Überarbeitung
1.0	15.02.2009	W. Bohn	Finale Version
2.0	30.04.2010	W. Bohn	Inhalt- und Layoutanpassung
2.1	21.12.2010	W. Bohn	Inhaltliche Anpassung
2.2	07.01.2011	W. Bohn	Inhaltliche Anpassung
2.3	20.01.2011	W. Bohn	Inhaltliche Anpassung
2.4	27.01.2011	W. Bohn	Inhaltliche Anpassung
2.5	04.02.2013	W. Bohn	Inhaltliche Anpassung
2.6	10.04.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

1 Allgemeines

Dieses Dokument beschreibt die Requesterzeugung sowie die Einbindung der Zertifikate im Microsoft IIS 7.0 Webserver. Der Ablauf im IIS 7.5 erfolgt analog.

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 des Zertifikats 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 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: https://www.telesec.de → ServerPass → Support

Hier gezeigt wird die Beauftragung eines ServerPass unter Verwendung des Produkts „TeleSec 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: https://www.telesec.de → ServerPass → Support → Root- / Sub-CA-Zertifikate

Hier werden ebenfalls alle relevanten Details wie Seriennummern, Laufzeiten, 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.

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 Microsoft IIS 7.0 Webserver

Die Beschreibung bezieht sich auf folgende Softwarekonstellation:

Microsoft Internet Information Server 7.0, deutsch
Microsoft Server 2008 R2 Standard, deutsch
Adobe Acrobat Reader 9, deutsch

Voraussetzung: Der Webserver startet bereits im unverschlüsselten Modus

Vor dem Import des Serverzertifikats ist ggf. der Import des CA-Zertifikats und evtl. auch des Root-Zertifikats erforderlich.

Die Einbindung von Root- und CA-Zertifikaten wird beschrieben in der Anleitung: „Microsoft Internet Information Server (IIS) V7.0“→ „Installation der CA-Zertifikate im IIS 7.0“

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

2 Requesterzeugung, Beauftragung, Installation, Sicherung des privaten Schlüssels

Während der Requesterzeugung werden die einzelnen Zertifikatsfelder abgefragt.

Alle hier eingetragenen Angaben erscheinen später unverändert im Zertifikat, im Einzelnen sind dies:

Beschreibung der Zertifikatseinträge:

„Gemeinsamer Name“	(*, 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 Organisationseinheit, 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: https://www.telesec.de/serverpass/support/downloadbereich/category/20-certification-practice-statement-cps

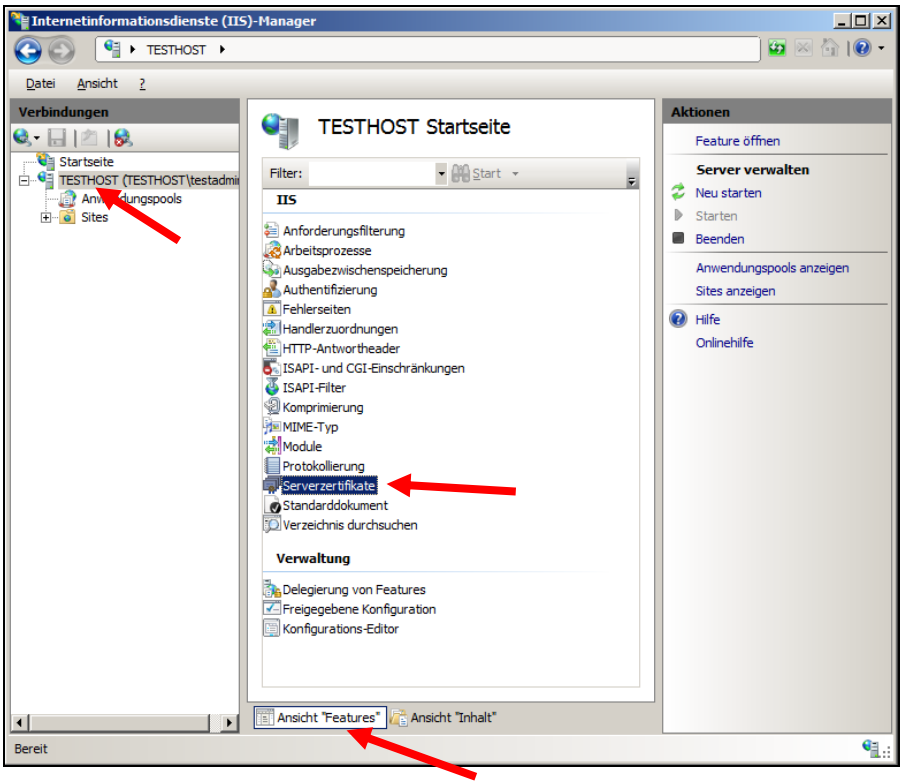
Vermeiden Sie die Verwendung von Feldern, die lediglich ein Leerzeichen enthalten!

2.1 Requesterzeugung

Zunächst öffnen Sie den Internetinformationsdienste-Manager, siehe Abb.1.
Diesen erreichen Sie über:

Start → Verwaltung → Internetinformationsdienste-Manager

Abbildung 1



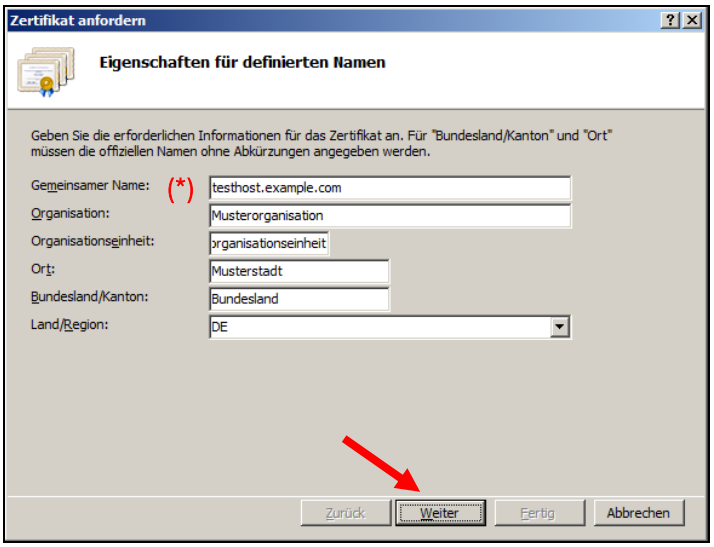
Im linken Fenster „**Verbindungen**“ wählen Sie Ihren Webserver aus, ggf. aktivieren Sie im mittleren Fenster die Option Ansicht „**Features**“. Nun wählen Sie im mittleren Fenster den Eintrag „**Serverzertifikate**“ durch Doppelklick aus, es erscheint Abbildung 3.

In dieser Anleitung trägt der Server die Bezeichnung „TESTHOST“, die Bezeichnung Ihres Servers wird abweichen!

Abbildung 3

Unter Aktionen wählen Sie die Option „**Zertifikatanforderung erstellen**“, es erscheint Abbildung 4.

Abbildung 4



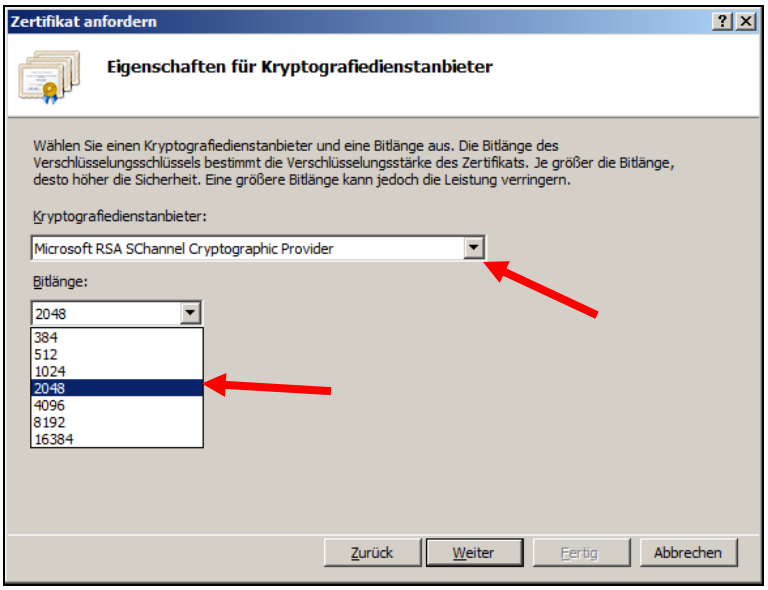
Wie in Abbildung 4, „Eigenschaften für definierten Namen“, dargestellt, werden die Zertifikatsangaben festgelegt. Füllen Sie die Felder entsprechend Ihrer Vorgaben aus.

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 6.

Abbildung 6

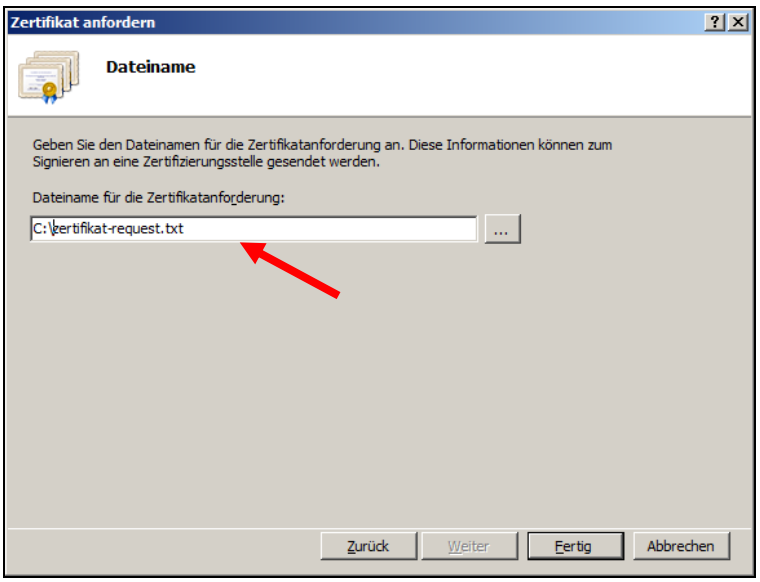


In Abbildung 6 werden die Eigenschaften für Kryptografiedienstanbieter festgelegt.
Unter Kryptografiedienstanbieter wählen Sie „Microsoft RSA SChannel Cryptographic Provider“.
Unter Bitlänge wird die verwendete Bitlänge (Schlüssellänge) festgelegt. Je nach verwendeter Version des IIS können mehrere Bitlängen ausgewählt werden.

Empfohlen wird eine Bitlänge von 2048 Bit. Requests mit einer Bitlänge kleiner 2048 Bit gelten nicht länger als sicher und sind von der Beauftragung ausgeschlossen

Die Festlegung einer noch höheren Bitlänge ist nicht erforderlich.
Über den Button **Weiter** gelangen Sie zu Abbildung 7.

Abbildung 7



In Abbildung 7 legen Sie den Pfad sowie einen Dateinamen für die Requestdatei fest, z. B. c:\zertifikat-request.pem.
Durch Drücken des Button **Fertig** wird die Requesterzeugung abgeschlossen.

Öffnen Sie die Requestdatei z. B. mit dem Windows Editor, sie erreichen ihn über:

Start → Alle Programme → Zubehör → Editor

Der Request stellt sich dar, wie in Abbildung 8 angegeben.

Abbildung 8 (zertifikat-request.txt)

```
—BEGIN NEW CERTIFICATE REQUEST—
IUHILHJKGUTUGHJOILUOJHKLJLUOHJKHHLKKLHKKLHKLHKLU
JHKHKKJLJKHKJHJKHJK786765HJKHKJHJKHJKHJKHJKHJKJK
.....
KLMKLPZQW4onheuHZIIO5BugGDRDZ878GJHKFDRTSXY45dfdgfjj5677
—END NEW CERTIFIQATE REQUEST—
```

2.2 Beauftragung des Serverzertifikats

Nachdem der Request erzeugt wurde, können Sie auf unserer Internetseite einen Server-Pass 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 8, inklusive der „----BEGIN.... und ----END... “ Zeilen, per cut & paste.

Nach dem Einfügen wird der Request automatisch einer Kontrolle unterzogen und die ermittelten Inhalte gemäß Abbildung 9 angezeigt.
Sollte ein Fehler festgestellt werden, erfolgt ein entsprechender Hinweis.

Abbildung 9

Füllen Sie alle weiteren Felder entsprechen Ihrer Vorgaben aus und senden den Online-Auftrag ab.
Das Auftragsformular 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 des Server-Zertifikats

Achtung: Vor der Installation des Serverzertifikats ist der Import der ausstellenden Instanzen (CA-Zertifikat und ggf. auch das Root-Zertifikat) erforderlich.
Hierzu ist eine separate Anleitung im Support Bereich verfügbar.
https://www.telesec.de/serverpass/ → ServerPass → Support → Downloadbereich → Anleitungen
Hier wählen Sie „Installation der CA-Zertifikate“.

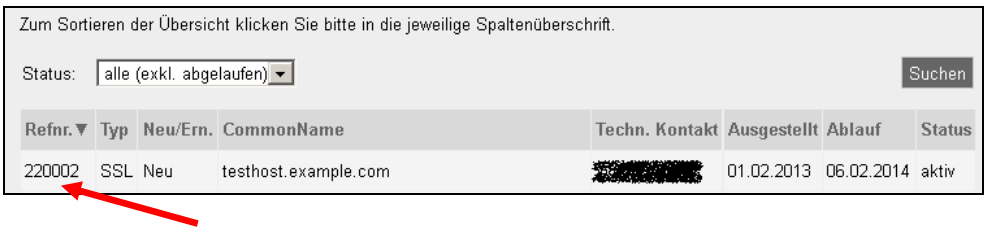
2.3.1 Herunterladen des Server-Zertifikats

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

Wählen Sie den Menüpunkt „Meine Zertifikate“

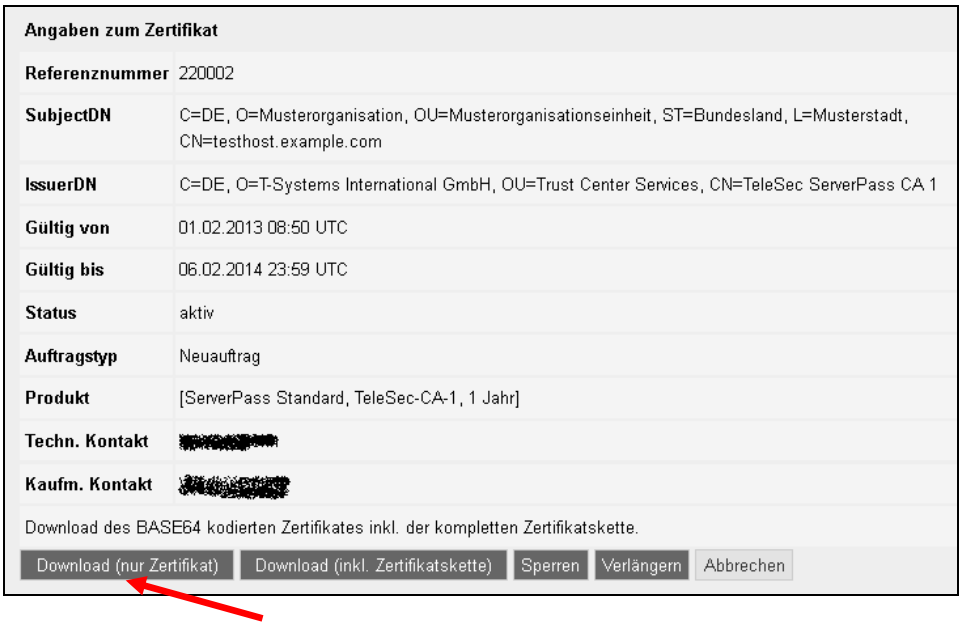
Hier werden nun alle Ihre Zertifikate aufgelistet.
Wählen Sie das herunterzuladende Zertifikat durch Klick auf die Referenznummer aus, siehe Abbildung 10.

Abbildung 10:



Es werden zwei Download-Formate angeboten, siehe auch Abbildung 11:
- Download (Nur Zertifikat)
- Download (inkl. Zertifikatskette)

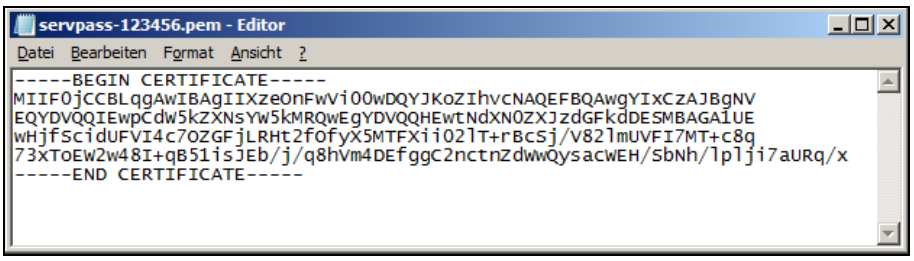
Abbildung 11



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 heruntergeladene Datei enthält das Server-Zertifikat, wie in Abbildung 12 dargestellt.

Abbildung 12 (servpass-123456.pem)



2.3.2 Import des Serverzertifikats

Falls noch nicht geschehen, so müssen zunächst die Zertifikate der ausstellenden Instanzen importiert werden. Hierfür ist eine separate Anleitung verfügbar. Sie finden die Anleitung auf unserer Internetseite unter „Support“.

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

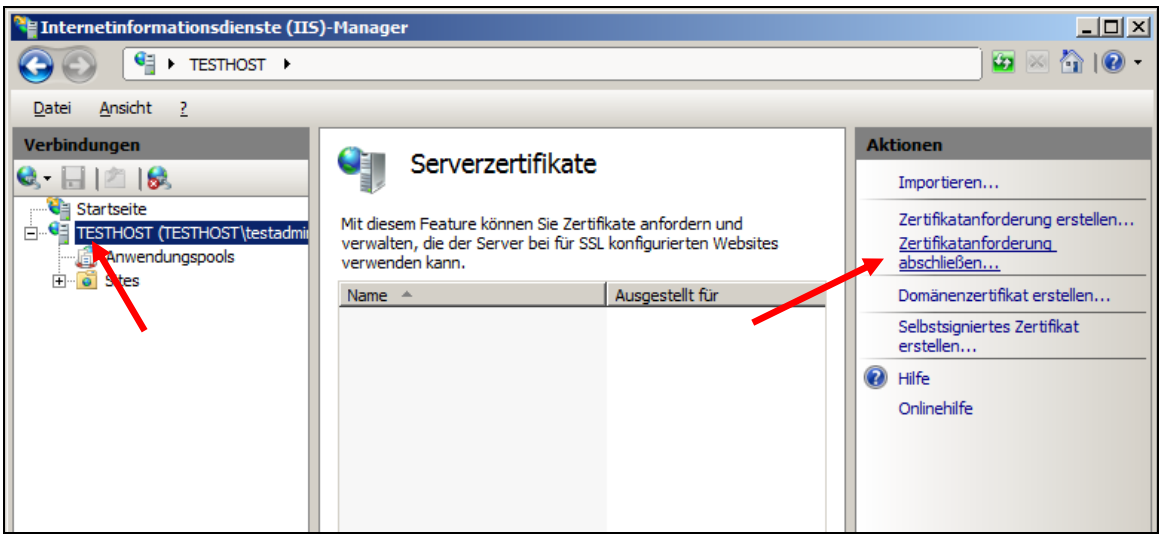
Import des Serverzertifikats

Öffnen Sie den Internet Informationsdienste-Manager, siehe Abb.1. Diesen erreichen Sie über:

Start → Verwaltung → Internetinformationsdienste-Manager

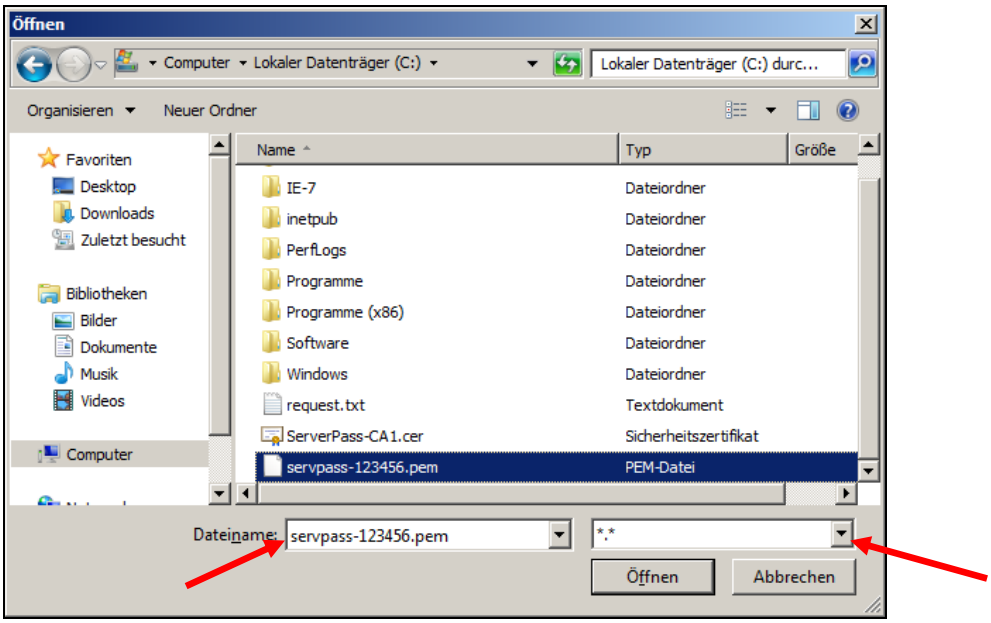
Im linken Fenster „**Verbindungen**“ wählen Sie Ihren Webserver aus, ggf. aktivieren Sie im mittleren Fenster die Option Ansicht „**Features**“. Nun im mittleren Fenster den Eintrag „**Serverzertifikate**“ per Doppelklick aufrufen, es erscheint Abbildung 13.

Abbildung 13



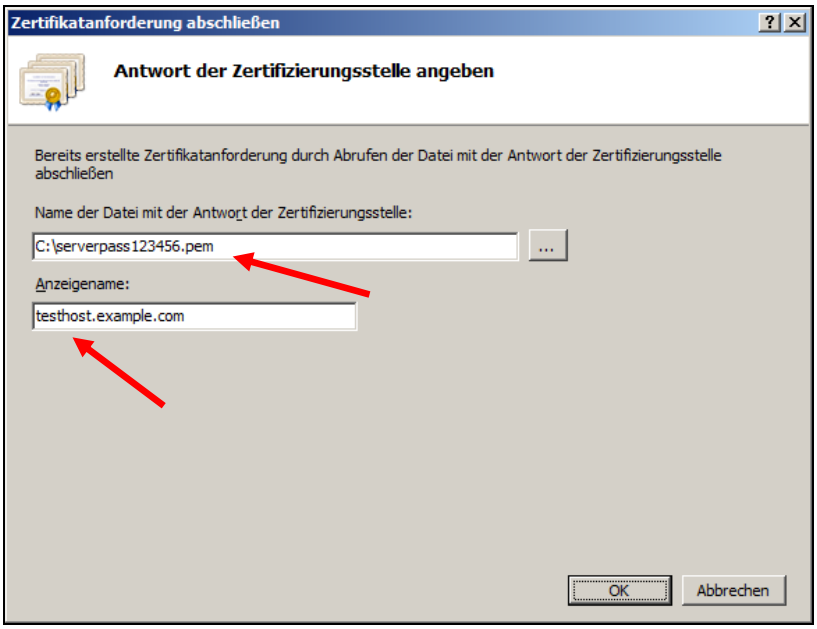
Hier wählen Sie unter „**Aktionen**“ nun den Eintrag „**Zertifizierungsanforderung abschließen**“, es öffnet sich Abbildung 14.

Abbildung 14:



Legen Sie den Pfad zu der Zertifikatsdatei fest, ggf. muss der Dateisuffix per Dropdown eingestellt werden auf die Auswahl aller Dateien: „***.***“.
Durch Drücken auf „**Öffnen“** gelangen Sie zu Abbildung 15.

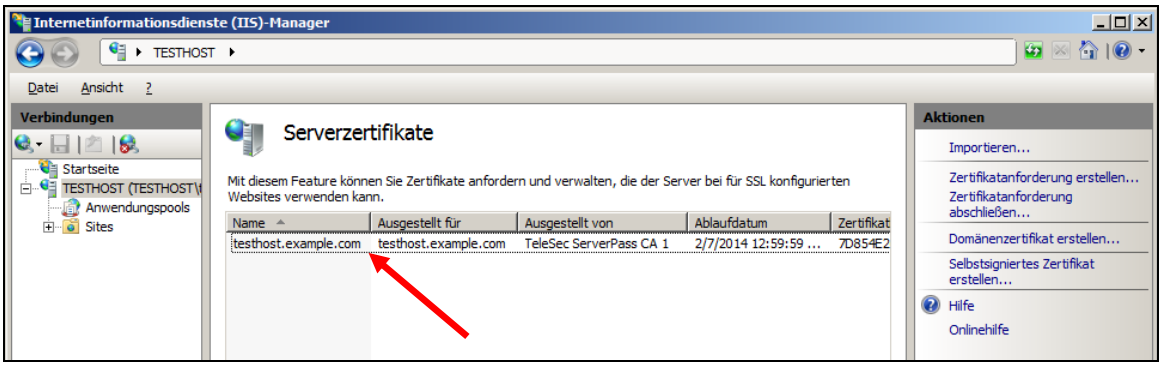
Abbildung 15:



In Abbildung 15 „Antwort der Zertfizierungsstelle angeben“ erscheint nun der Name der Datei mit der Antwort der Zertifizierungsstelle.

Im Feld „**Anzeigename**“ legen Sie eine Bezeichnung fest, unter der das Zertifikat später in der Zertifikatsverwaltung angezeigt wird. Im Beispiel haben wir die Bezeichnung „testhost.example.com“ gewählt. Durch Drücken auf „**OK“** wird der Import abgeschlossen. Der Import dauert mitunter eine Minute.

Abbildung 16:



Das importierte Zertifikat wird aufgelistet, wie in Abbildung 16 dargestellt.

2.4 Konfiguration des SSL-Modus

Der Webserver wird nun für den Einsatz des Zertifikats im SSL-Modus konfiguriert.

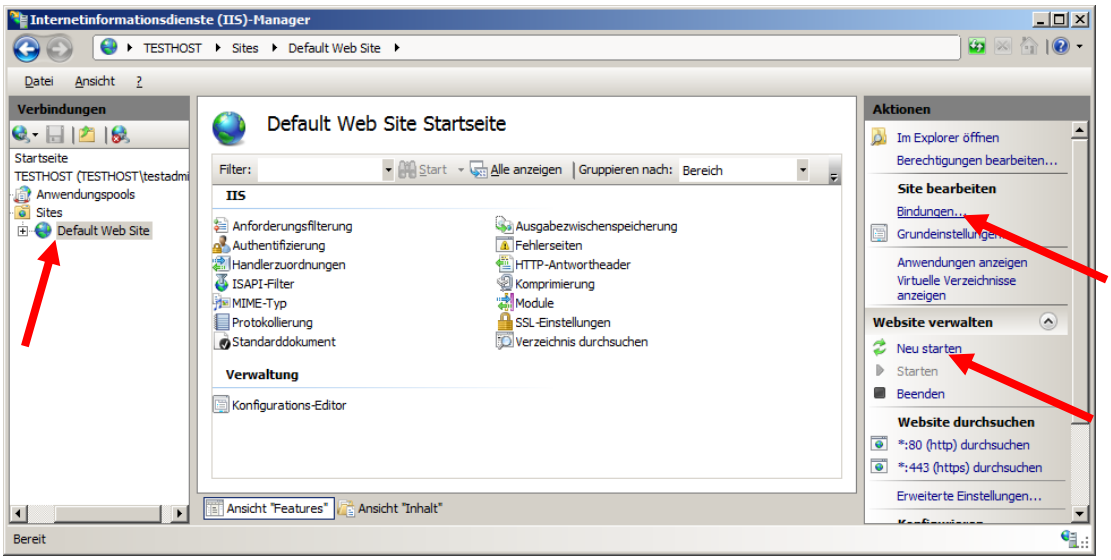
Öffnen Sie den Internet Informationsdienste-Manager:

Start → **Systemsteuerung** → **Verwaltung** → **Internetinformationsdienste**.

Unter **Verbindungen** wählen Sie „**Servername (Servername\Administrator)** → **Sites** → **Default Web Site**

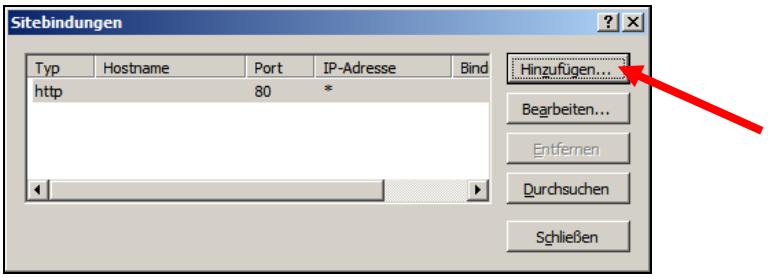
Im Fenster „**Aktionen**“ wählen Sie nun unter „**Site bearbeiten**“ die Option „**Bindungen**“ bzw. „**Bindungen bearbeiten**“, siehe Abbildung 17.

Abbildung 17



Sie gelangen zum Dialog „Sitebindungen“, siehe Abbildung 18.

Abbildung 18:



Liegt noch kein Eintrag für https vor, muss nun eine Verbindung hinzugefügt werden, wählen Sie „**Hinzufügen**“.
Falls schon ein Eintrag für https existiert, markieren Sie diesen Eintrag und drücken auf „**Bearbeiten**“.

Abbildung 19

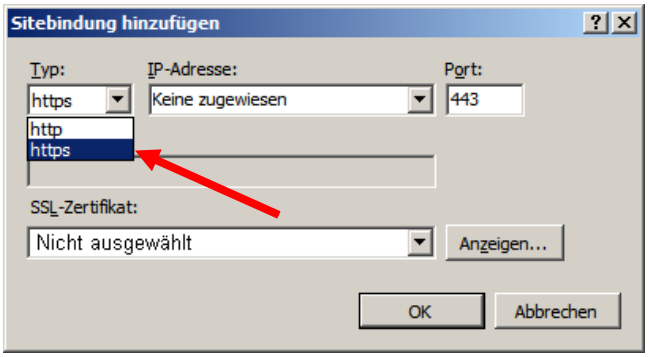
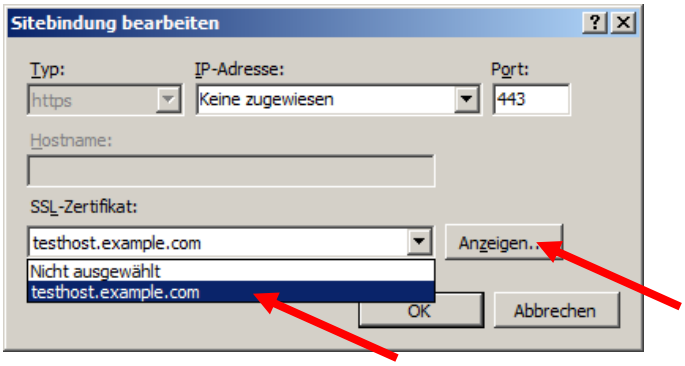


Abbildung 19: Festlegung der Parameter für den SSL-Modus:
Als Typ wird „**https**“ verwendet
Unter **IP-Adresse** wählen Sie standardmäßig „**Keine zugewiesen**“.
Als Port wird standardmäßig „**443**“ verwendet.
Weitere Hinweise zu diesen Feldern entnehmen Sie bitte der Windows-Hilfe. Sie erreichen die Hilfe über die Taste „F1“.
Unter **SSL-Zertifikat** wählen Sie im Dropdown-Menü Ihr zuvor importiertes Zertifikat aus.

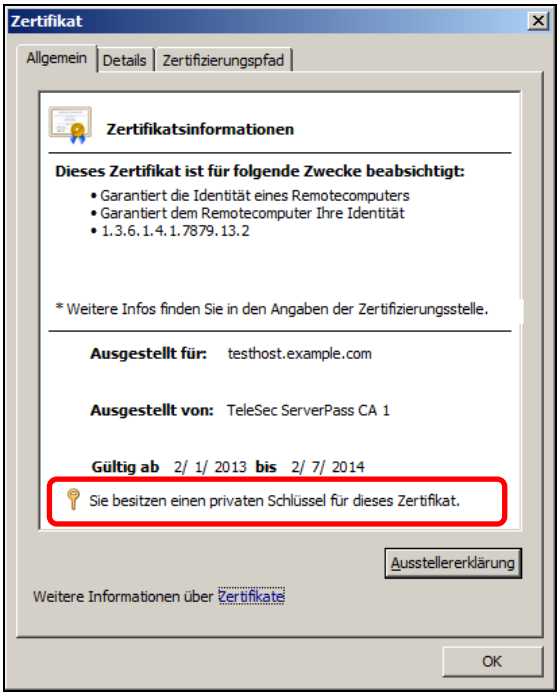
Sind mehrere Zertifikate vorhanden, so werden diese im Dropdown-Menü angezeigt, siehe Abbildung 20.

Abbildung 20



Um das zuvor importierte Zertifikat zu ermitteln, markieren Sie zunächst ein Zertifikat aus der DropDown-Liste. Über den Button „**Anzeigen**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 21.

Abbildung 21



Achten Sie hier auf die korrekten Angaben für die Gültigkeit, „Ausgestellt für“ und „Aufgestellt von“!
Wichtig: Der Hinweis: „Sie besitzen einen privaten Schlüssel für dieses Zertifikat“ muss erscheinen, ansonsten können Sie dieses Zertifikat nicht für die SSL-Verschlüsselung nutzen!
Weitere Zertifikatsangaben erreichen Sie über den Reiter **Details**.

Nach Auswahl des korrekten Zertifikats wird die Einstellung durch drücken von **OK** übernommen. Die Übernahme dauert bisweilen eine Minute.

Die Installation des Serverzertifikates ist nun abgeschlossen.

Nachdem der Webserver bzw. die Webseite neu gestartet wurde, können verschlüsselte Verbindungen über https aufgebaut werden.

Einen Neustart der Webseite veranlassen Sie z. B. über den Server-Manager:
Server-Manager → Internetinformationsdienste
Unter „Verbindungen“ wählen Sie:
„TESTHOST“ (bzw. die Bezeichnung Ihres Webservers), dann „Sites“ und schließlich die per Zertifikat geschützte Webseite, z. B. **Default Web Site**.
Im Menü **Website verwalten** wählen Sie **Neu starten**, siehe Abbildung 17.

Nach dem Neustart können Sie den Servermanager beenden und die geschützte Webseite kontrollieren, siehe Punkt 3 bzw. zunächst eine Sicherheitskopie des Serverschlüssels erzeugen, siehe 2.5.:

Es wird dringend empfohlen, den erzeugten Serverschlüssel zu sichern!

2.5 Sicherung des Serverschlüssels incl. Serverzertifikat

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

Öffnen Sie den Internet Informationsdienste-Manager:

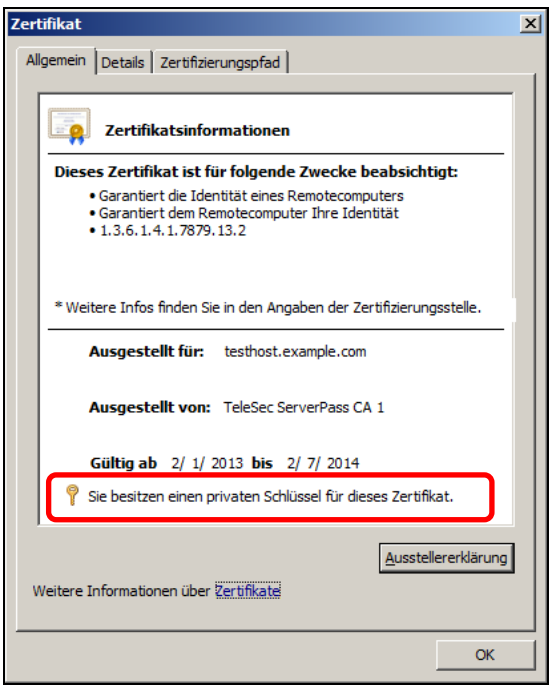
Start → Systemsteuerung → Verwaltung → Internetinformationsdienste.

Unter „**Verbindungen**“ wählen Sie „**Servername (Servername\Administrator)“**
Nun wählen Sie den Eintrag „**Serverzertifikate**“ per Doppelklick aus, es erscheint Abbildung 22.

Abbildung 22

Unter „**Serverzertifikate**“ wählen Sie nun das zu sichernde Zertifikat per Doppelklick aus, es erscheint Abbildung 23.

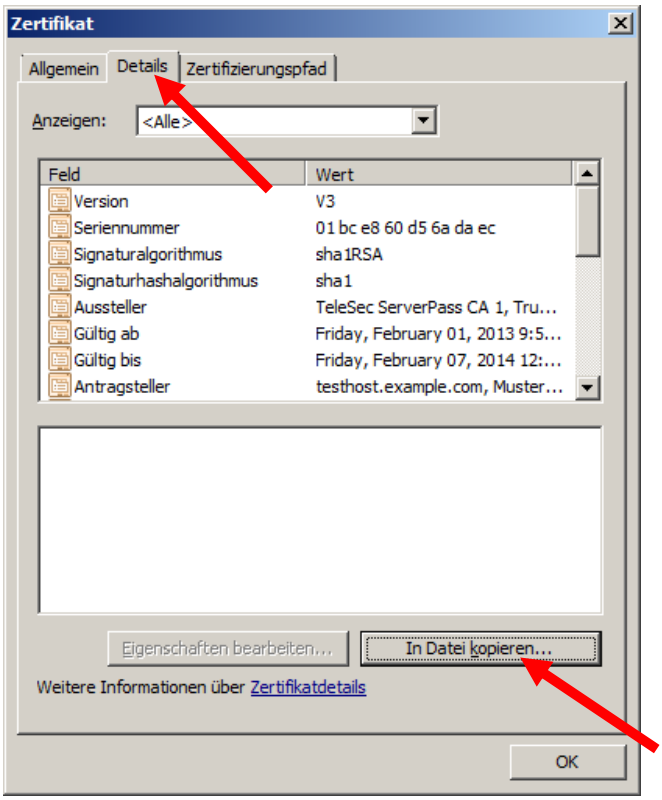
Abbildung 23



Achten Sie hier auf die korrekten Angaben für die Gültigkeit, „Ausgestellt für“ und „Aufgestellt von“, sowie auf den Hinweis: „Sie besitzen einen privaten Schlüssel für dieses Zertifikat“.

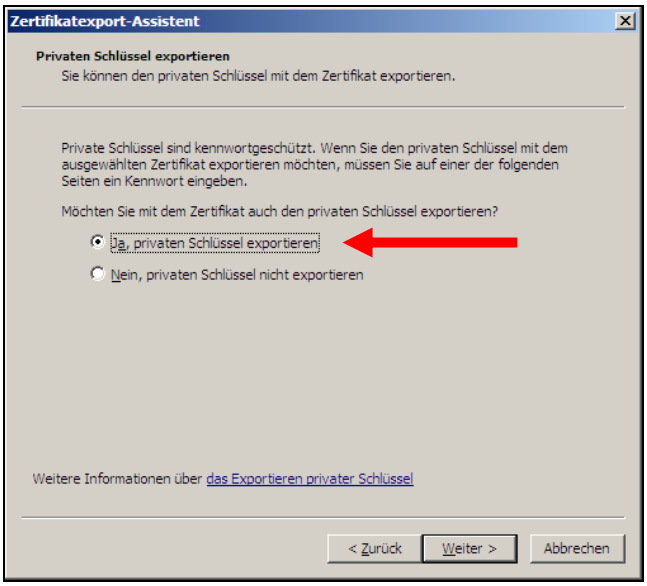
Wählen Sie den Reiter **Details**, es erscheint Abbildung 24.

Abbildung 24



Wählen Sie: „**In Datei Kopieren**“, es öffnet sich der Zertifikatexport-Assistent, siehe Abbildung 25.

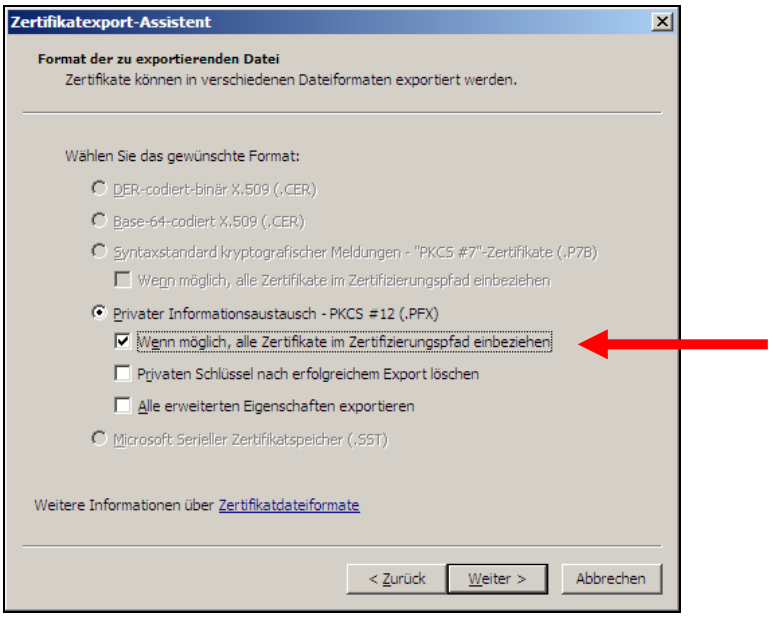
Abbildung 25:



Im Dialogfenster **Privaten Schlüssel exportieren** wählen Sie:

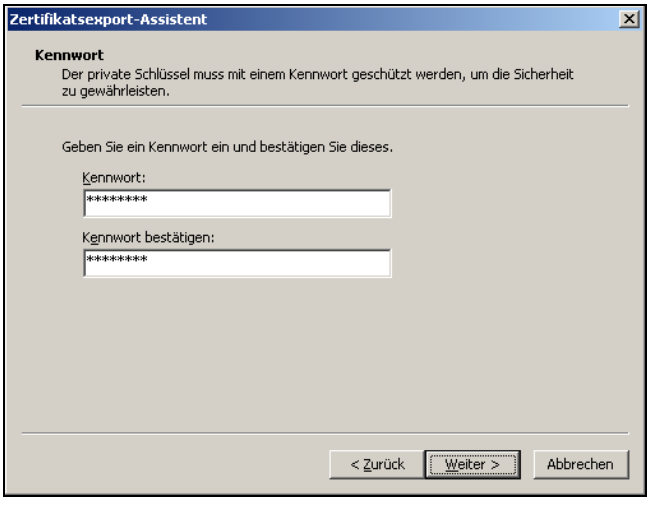
„Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?“
„Ja, privaten Schlüssel exportieren“. Klicken auf „**Weiter**“.

Abbildung 26:



Im Dialogfenster „Format der exportierenden Datei“ wählen Sie:
Privater Informationsaustausch – PKCS #12 (.pfx)
Aktivieren Sie lediglich die Option **Wenn möglich alle Zertifikate im Zertifizierungspfad einbeziehen**.

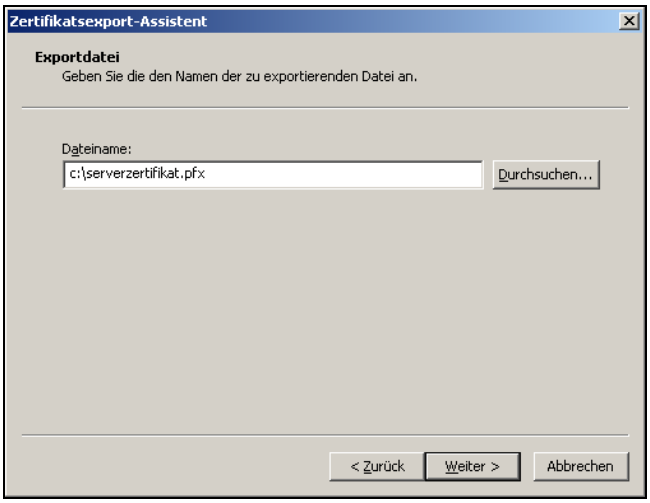
Abbildung 27:



Im Dialogfenster „Kennwort“ wird ein Passwort für den exportierten Schlüssel festgelegt.

Achtung: Dieses Passwort wird bei einem ggf. erforderlichen Import benötigt!

Abbildung 28:



Abschließend wird noch ein Dateiname bzw. der Speicherort für die Sicherungsdatei vergeben, z. B. c:\serverzertifikat.pfx.

Nach erfolgreichem Export können Sie die MMC-Konsole schließen.
Konsole → Datei → Beenden
Die evtl. erscheinende Meldung „**Konsole speichern?**“ quittieren sie mit „**Ja**“.

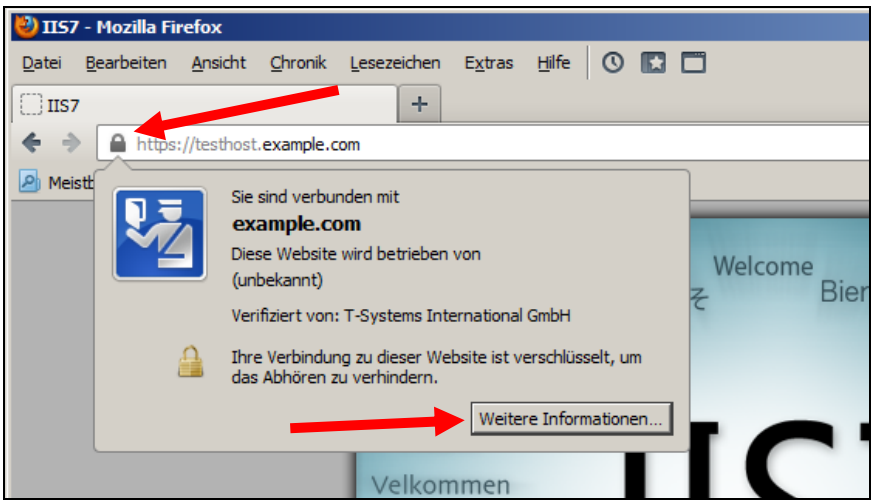
Der Vorgang ist hiermit abgeschlossen und Sie können den Servermanager nun beenden.

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.
Exemplarisch ist hier die Darstellung im Firefox (Abbildung 29-31) sowie im Internet Explorer (Abbildung 32-34) aufgeführt.
Andere Browser stellen den SSL-Modus ggf. anders dar.

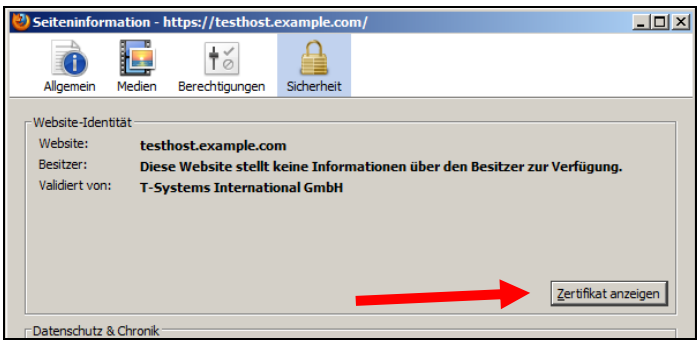
Firefox:

Abbildung 29 (Firefox 18):



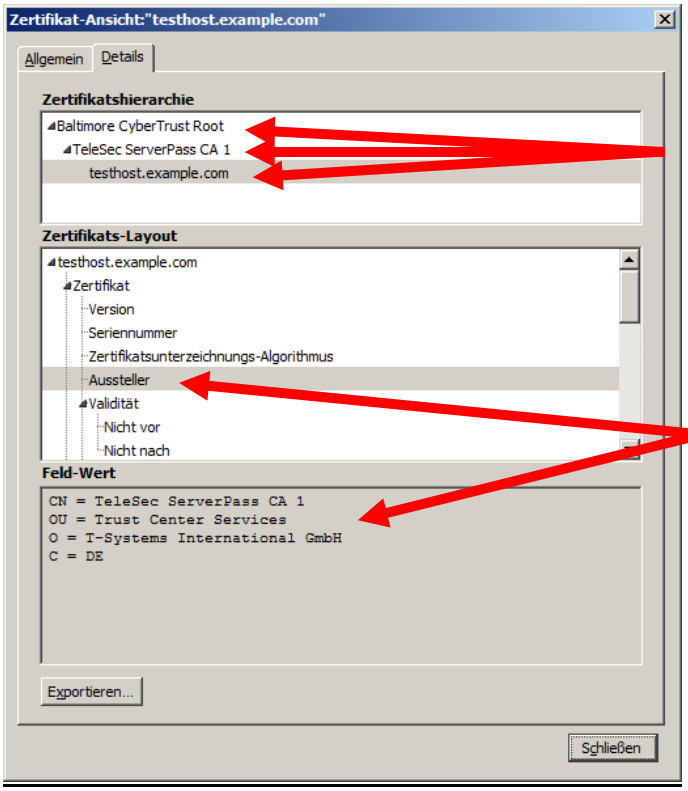
Beim Firefox lassen sich über einen Klick auf das Schloss Details zum verwendeten Zertifikat anzeigen.
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 30 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

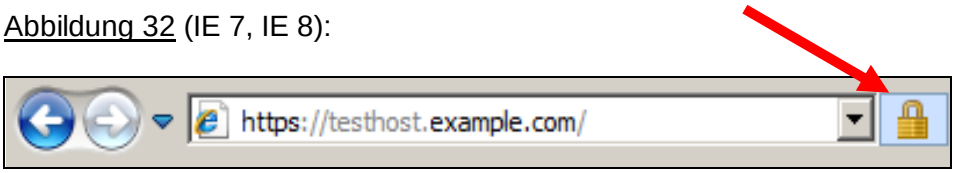
Abbildung 31 (Firefox 18):



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“

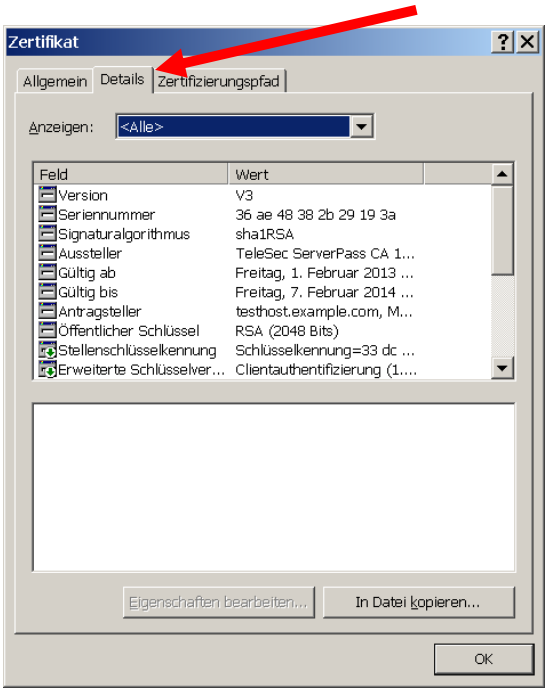
Internet Explorer

Abbildung 32 (IE 7, IE 8):



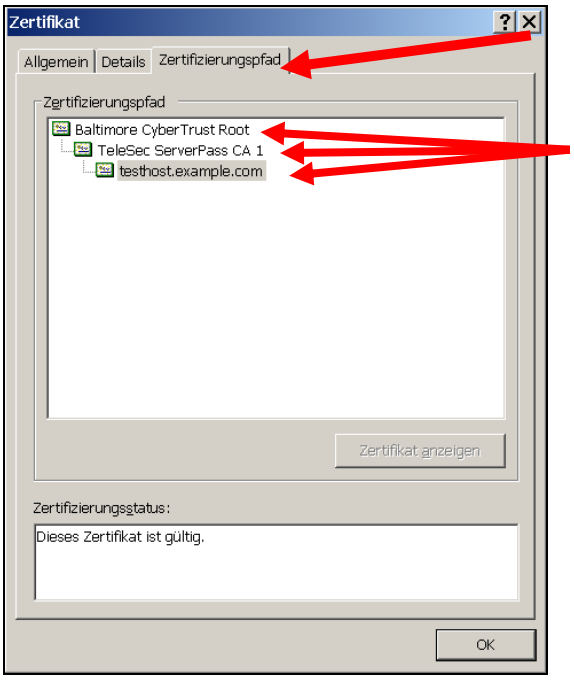
Beim Internet Explorer lassen sich die Zertifikatsdetails durch Doppelklick auf das Schloss anzeigen.
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 33.

Abbildung 33 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 34.

Abbildung 34 (Die Zertifikatskette)



Darstellung der kompletten Zertifikatskette

So wie in Abbildung 34 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.

Wird die Zertifikatskette nicht korrekt angezeigt, so muss das CA-Zertifikat im Webserver importiert werden, siehe hierzu Anleitung:

„Microsoft Internet Information Server (IIS) V7.0“ → „Installation der CA-Zertifikate im IIS 7.0“

http://www.telesec.de/serverpass/support_downloads.html