TeleSec ServerPass

Zertifikats-Erneuerung mit dem MS IIS 7.0

Version: 2.5
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_msiis_7.doc		Requesterzeugung Microsoft IIS 7.0 Webserver

Version	Stand	Status
2.5	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
Zertifikats-Erneuerung 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	30.11.2010	W. Bohn	Inhaltliche Anpassung
2.2	18.01.2011	W. Bohn	Inhaltliche Anpassung
2.3	27.01.2011	W. Bohn	Inhaltliche Anpassung
2.4	04.02.2013	W. Bohn	Inhaltliche Anpassung
2.5	10.4.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

1 Allgemeines

Dieses Dokument beschreibt die Zertifikatserneuerung 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 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 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.
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 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 Version 9, deutsch

Voraussetzung: Der Webserver läuft bereits im SSL-Modus unter Verwendung eines TeleSec ServerPass Serverzertifikats.

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 -> Anleitungen

2 Zertifikat erneuern

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

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

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

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

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 „Microsoft Internet Information Server (IIS) V7.0 Zertifikat-Requesterzeugung, Installation der Zertifikate“.

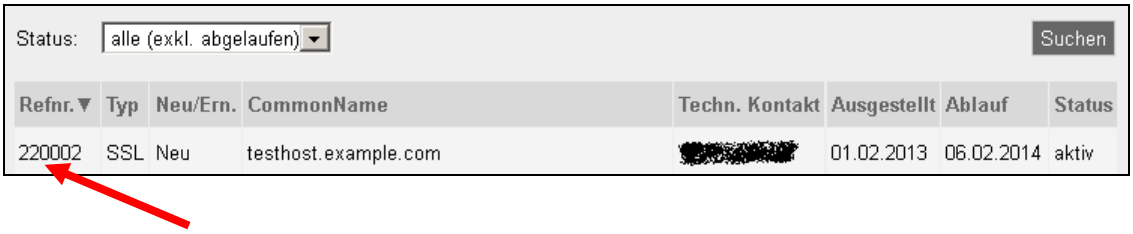
2.2 Besonderer Hinweis für eine Zertifikats-Erneuerung mit Microsoft IIS 7.0 Webserver

Man kann nicht die Erneuerungsfunktion des IIS-Managers verwenden, da hierbei ein Request mit lediglich 1024 Bit Schlüssellänge erzeugt wird.

In der Regel ist die Erzeugung eines weiteren Requests auch nicht erforderlich.
Sollte dennoch ein neuer Request erzeugt werden, so erzeugen Sie bitte eine neue Zertifikatsanforderung, gemäß Anleitung „Microsoft Internet Information Server (IIS) V7.0 -> 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.
Beim IIS 7.0 können problemlos mehrere Schlüssel bzw. Zertifikate parallel existieren.
Sie werden dann aufgelistet entsprechend Abbildung 14.

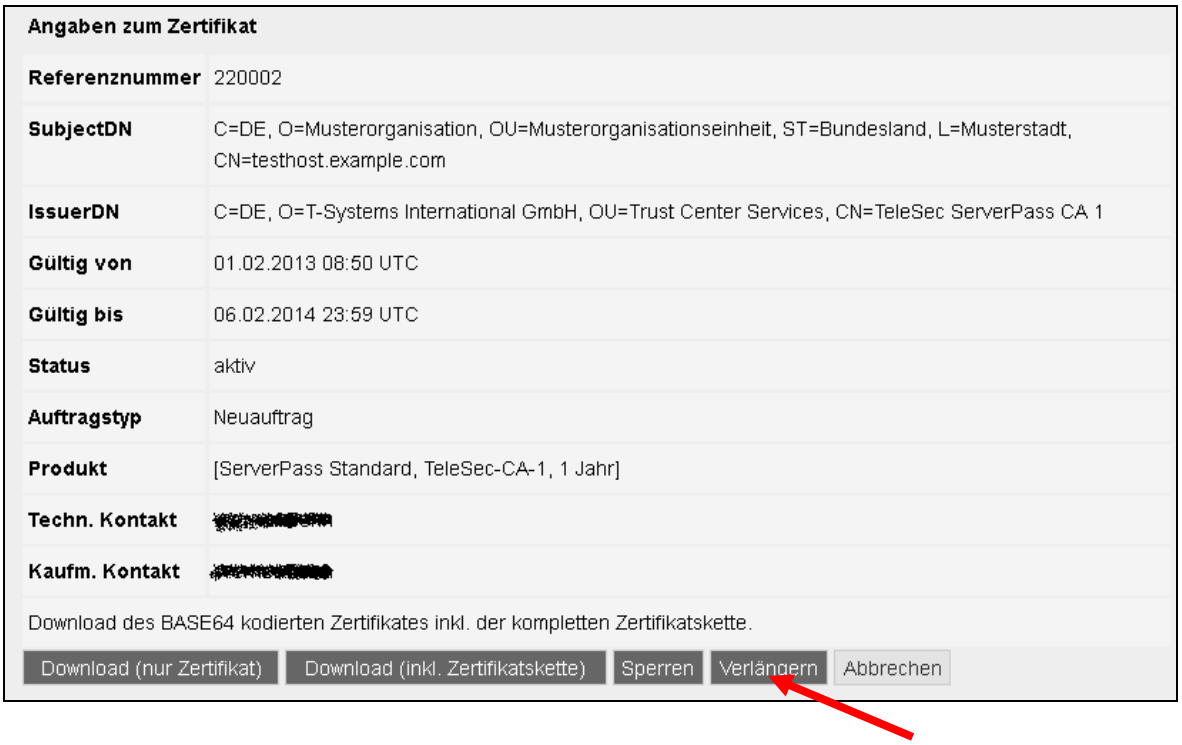
2.3 Erneuerung durchführen

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.

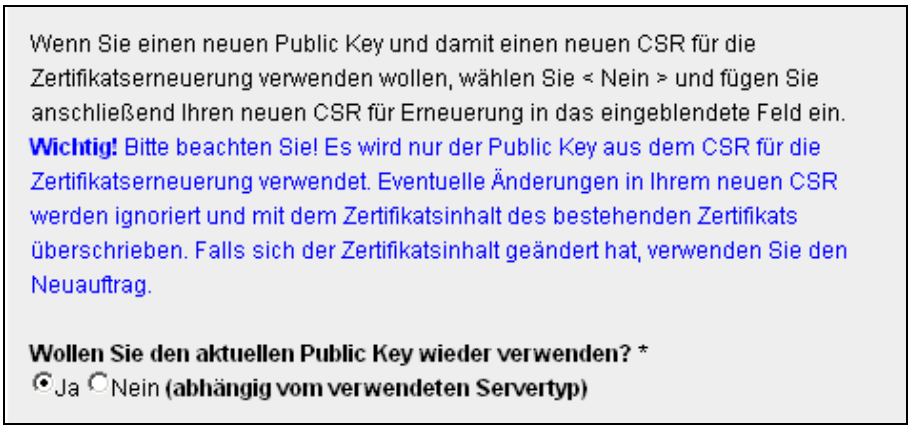
Abbildung 4:

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 und anschließend ein neuer Request erzeugt werden.

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

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

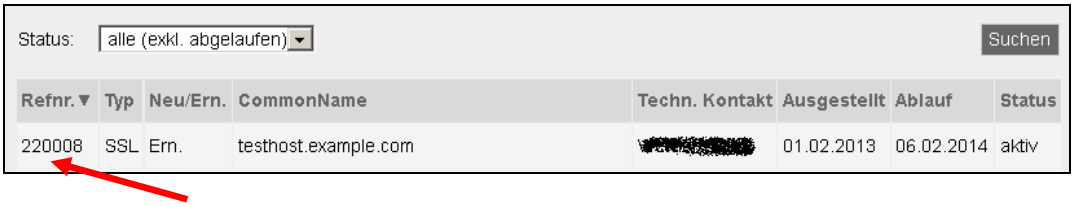
Wie beschrieben, lässt sich das Zertifikat aus dem vorangegangen Dialog herunterladen bzw. erst nach Anmeldung im Portal „myServerPass“:

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

Wählen Sie den Menüpunkt „Meine Zertifikate“

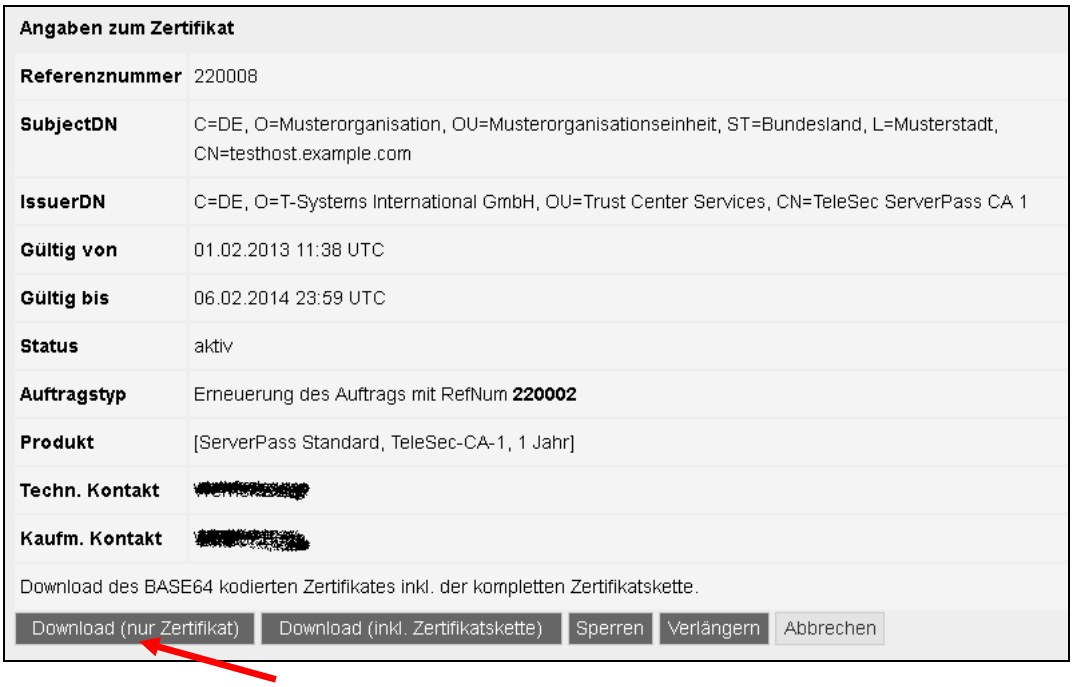
Hier werden nun alle Ihre Zertifikate aufgelistet, siehe Abbildung 8.

Abbildung 8



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

Abbildung 9



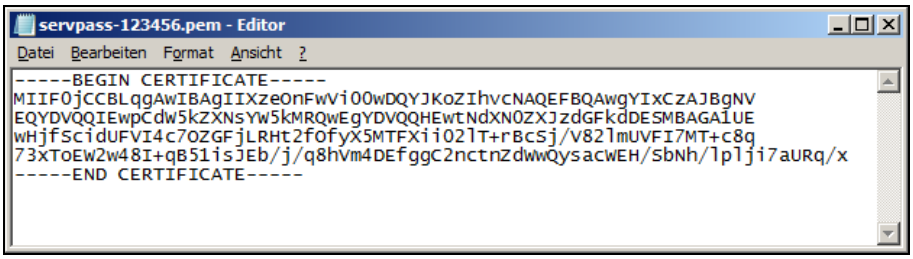
Wie in Abbildung 9 gezeigt, werden die Zertifikatsdaten zur Kontrolle angezeigt. Angeboten werden zwei Download-Formate:

- 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 den Internetinformationsdienste-Manager, siehe Abbildung1. Sie erreichen ihn über:

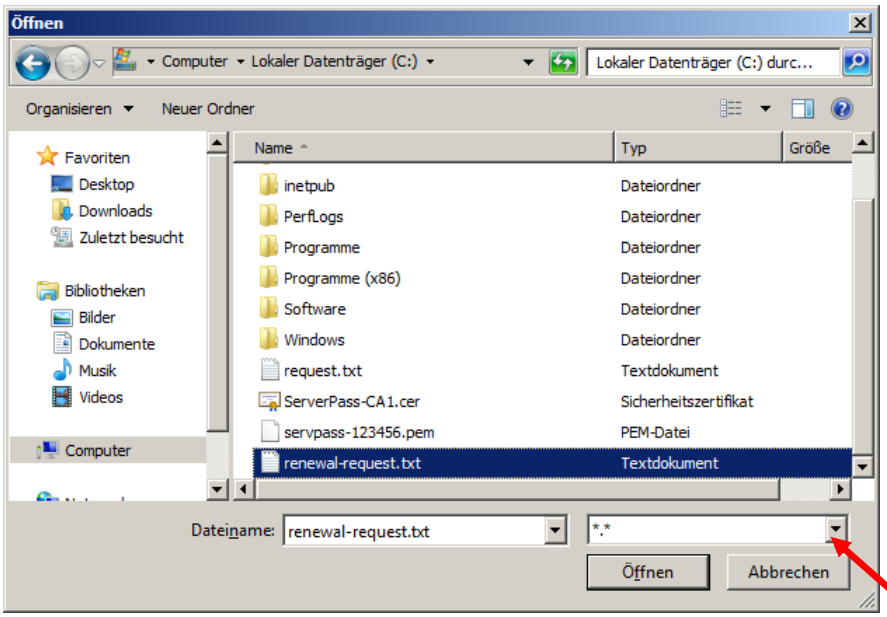
Start → Verwaltung → Internetinformationsdienste-Manager

Im linken Fenster „Verbindungen“ wählen Sie Ihren Webserver aus, ggf. aktivieren Sie im mittleren Fenster die Option Ansicht „Features“. Nun aktivieren Sie im mittleren Fenster den Eintrag „Serverzertifikate“ per Doppelklick, es erscheint Abbildung 11.

Abbildung 11

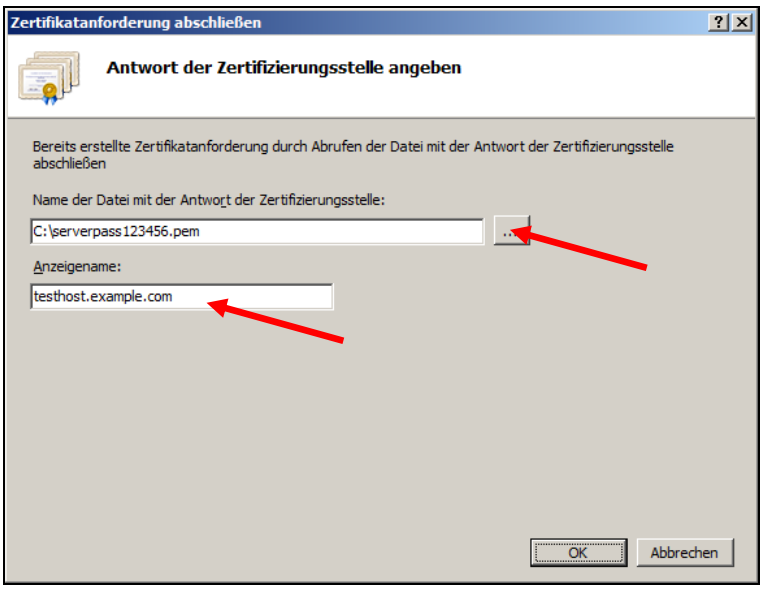
Hier wählen Sie unter „Aktionen“ nun den Eintrag „Zertifizierungsanforderung abschließen…“, es öffnet sich Abbildung 8.

Abbildung 8:



Legen Sie den Pfad zu der Zertifikatsdatei fest, ggf. muss das Dateisuffix per Dropdown eingestellt werden auf die Auswahl aller Dateien ***.***. Durch Drücken auf **„Öffnen“** gelangen Sie zu Abbildung 9.

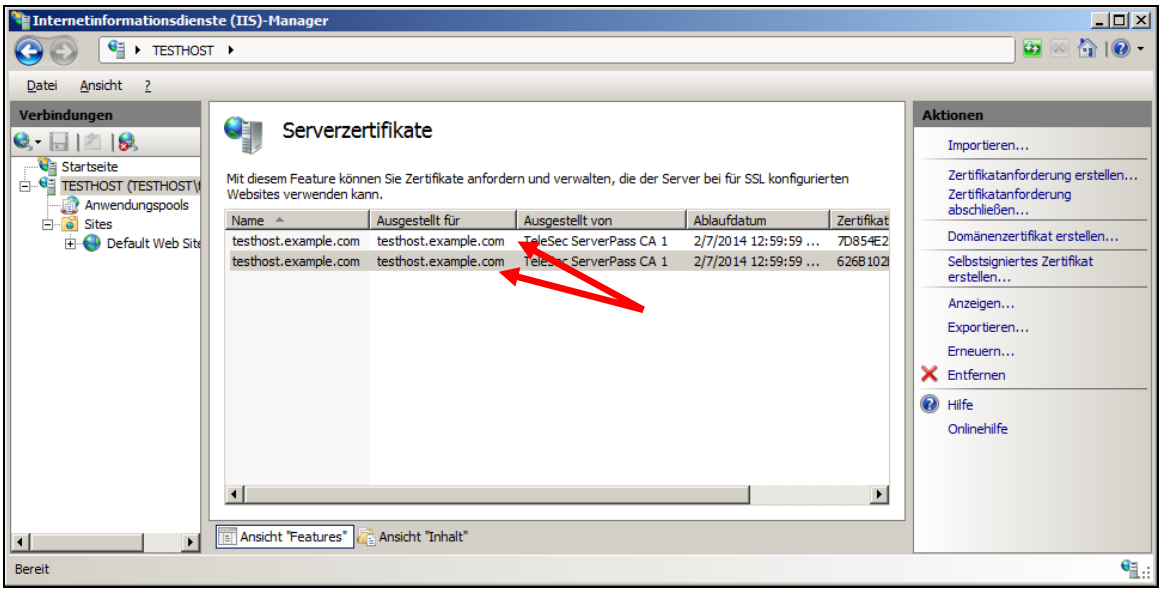
Abbildung 9:



Wie in Abbildung 9 „Antwort der Zertfizierungsstelle angeben“ erscheint nun der Name der zuvor herunter geladenen Datei.

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.

Abbildung 10:



Wie in Abbildung 10 dargestellt, wird das importierte Zertifikat jetzt unter dem bereits existierenden aufgelistet.

Nun muss der Webserver für Nutzung des neuen Zertifikats konfiguriert werden.

2.5 Verwendung des neuen Zertifikats

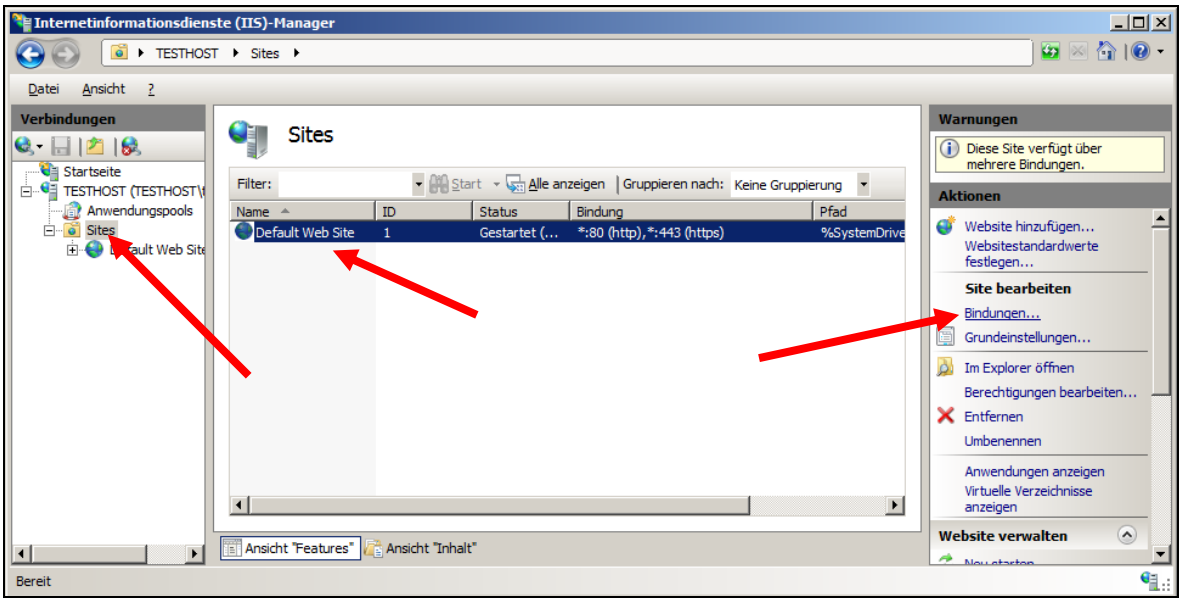
Der Webserver wird nun für den des neuen Zertifikats konfiguriert.

Öffnen Sie die Systemverwaltung:

Start → Systemsteuerung → Verwaltung → Internetinformationsdienste.

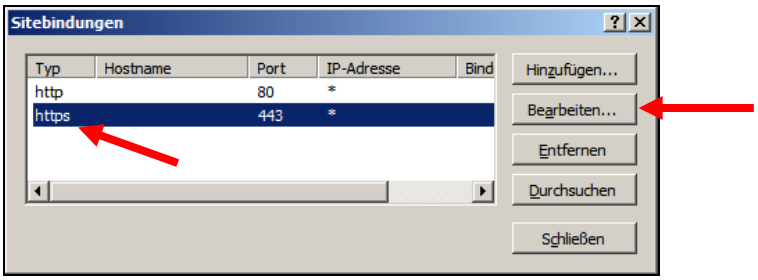
Unter „Verbindungen“ wählen Sie **Servername (Servername\Administrator) → Sites → Default Web Site**, siehe Abbildung 11.

Abbildung 11



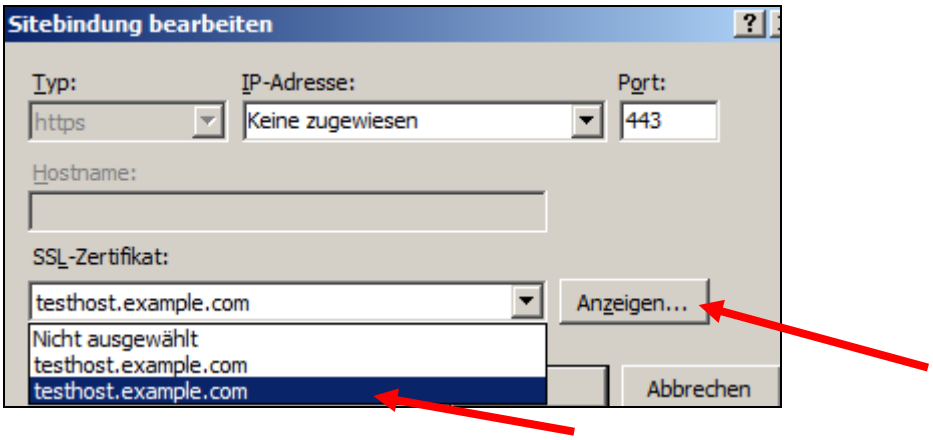
Im Fenster „Aktionen“ wählen Sie nun unter **Site bearbeiten** die Option **„Bindungen“** bzw. **„Bindungen bearbeiten“**.
Sie gelangen zum Dialog „Sitebindungen“, siehe Abbildung 12.

Abbildung 12:



Für die Verwendung des neuen Zertifikats muss die https-Verbindung bearbeitet werden, hierzu markieren Sie den Eintrag **„https“** drücken auf **„Bearbeiten“**.

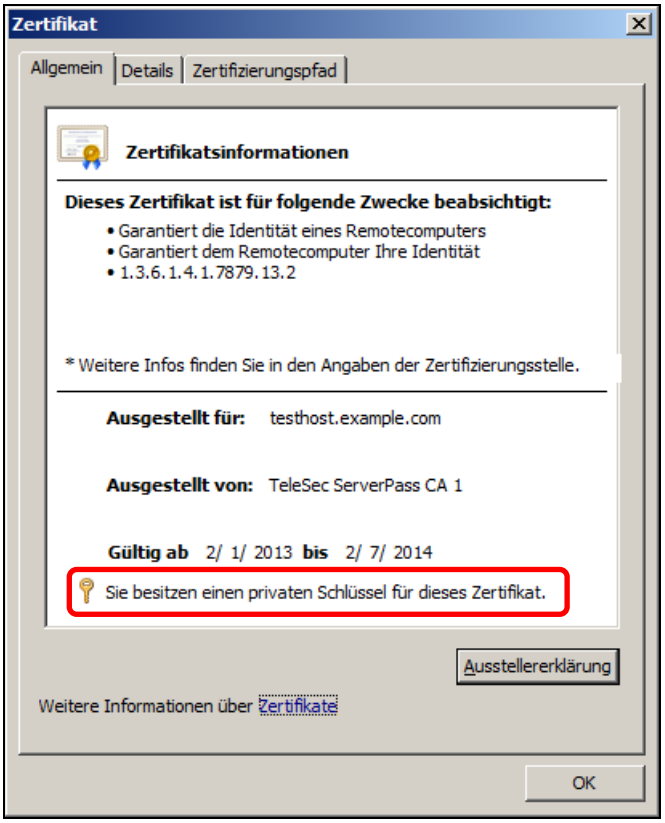
Abbildung 13



Unter **SSL-Zertifikat** wählen Sie im Dropdown-Menü Ihr zuvor importiertes Zertifikat aus, siehe Abbildung 13.

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 14.

Abbildung 14: (Zertifikatdetails)



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**“.

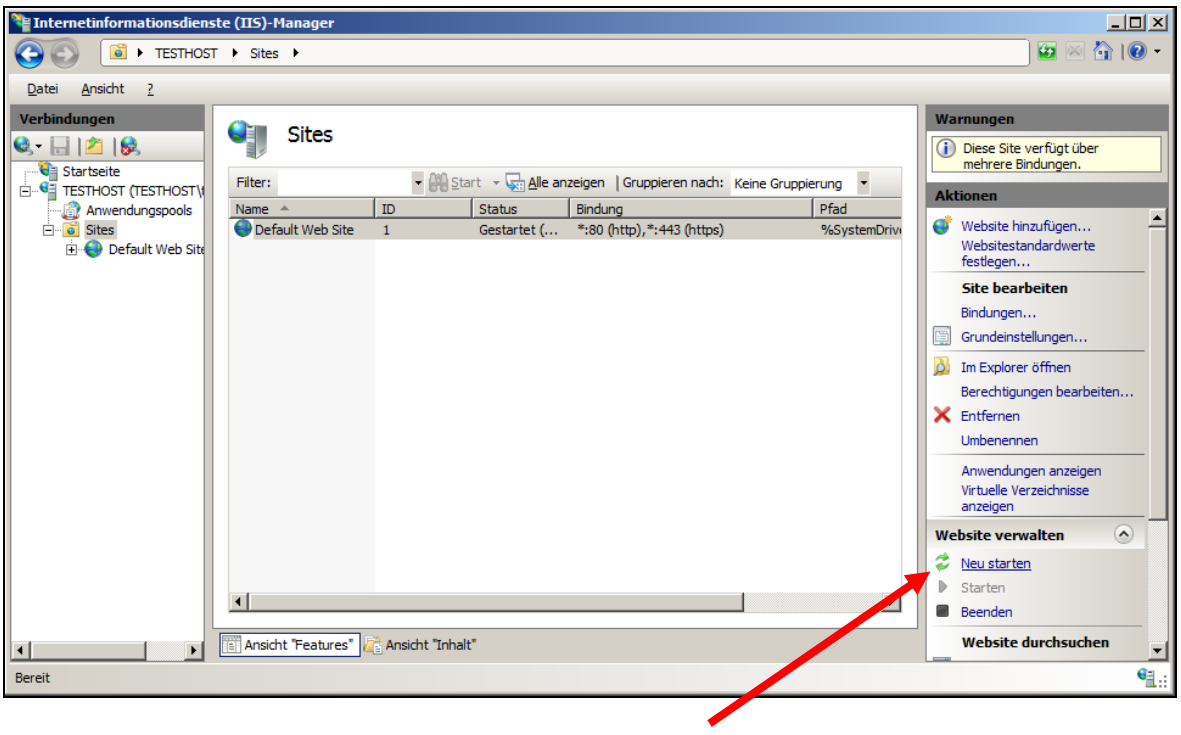
Nach Auswahl des korrekten Zertifikats wird die Einstellung durch Drücken von **„OK“** übernommen.

Die Installation des neuen Serverzertifikates ist nun abgeschlossen.

Nachdem der Web-Server neu gestartet wurde, können verschlüsselte Verbindungen über https aufgebaut werden.

Einen Neustart des Webservices veranlassen Sie z. B. über den Server-Manager:
Server-Manager → Internetinformationsdienste
Unter **„Verbindungen“** wählen Sie:
TESTHOST (bzw. die Bezeichnung Ihres Webservers)
Im Menü **Website verwalten** wählen Sie **„Neu starten“**, siehe auch Abbildung 15.

Abbildung 15: (Website neu starten)



Nach dem Neustart können Sie den Servermanager beenden und die geschützte Webseite kontrollieren, siehe Punkt 3 bzw. zunächst eine Sicherheitskopie des Serverschlüssels erzeugen, siehe 2.7:

Es wird dringend empfohlen, den erzeugten Serverschlüssel zu sichern!

2.6 Sicherung des Serverschlüssels incl. Serverzertifikat

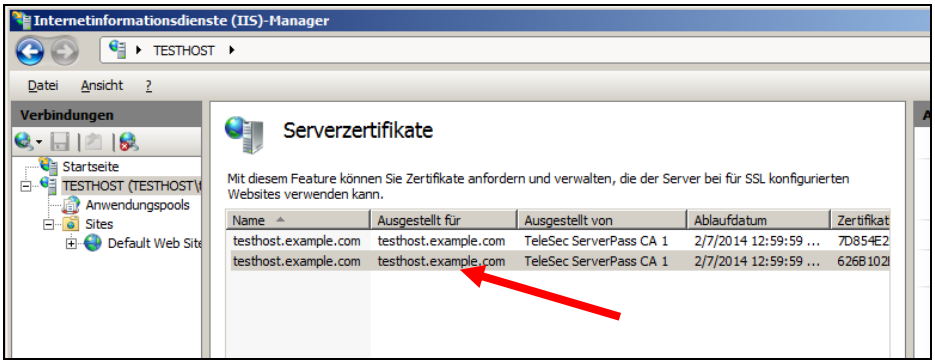
Es wird dringend empfohlen, die erzeugten Daten zu sichern, z. B. auf einem externen Medium.

Öffnen Sie den Internet Informationsdienste-Manager:

Start → Systemsteuerung → Verwaltung → Internetinformationsdienste.

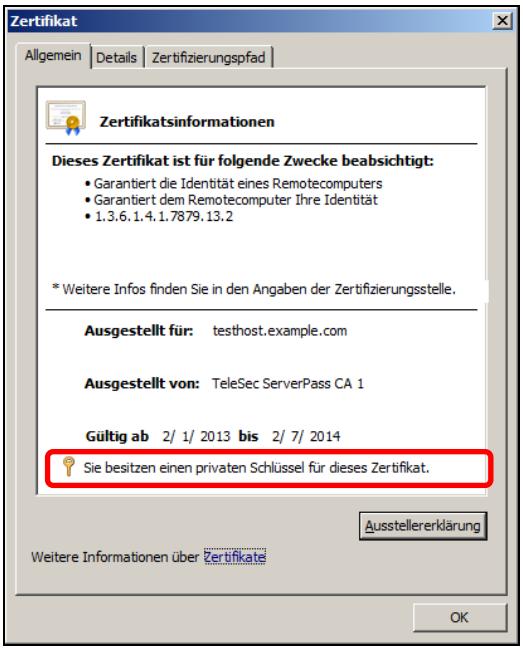
Unter „**Verbindungen**“ wählen Sie „**Servername (Servername\Administrator)“**
Nun wählen Sie den Eintrag „**Serverzertifikate**“ per Doppelklick aus, es erscheint Abbildung 16.

Abbildung 16



Unter „**Serverzertifikate**“ wählen Sie nun das zu sichernde Zertifikat per Doppelklick aus, es erscheint Abbildung 17.

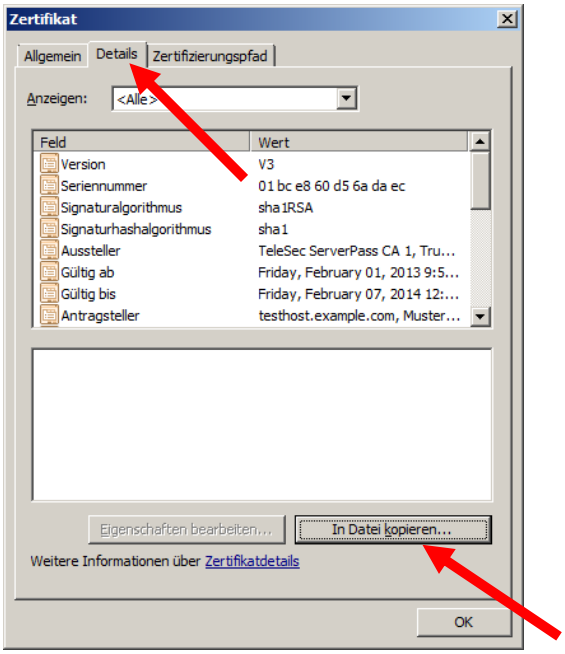
Abbildung 17



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“.

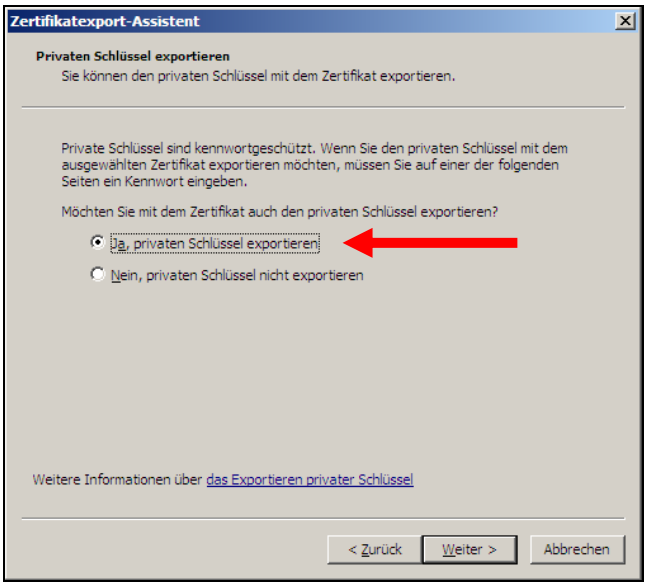
Wählen Sie den Reiter **Details**, es erscheint Abbildung 18.

Abbildung 18



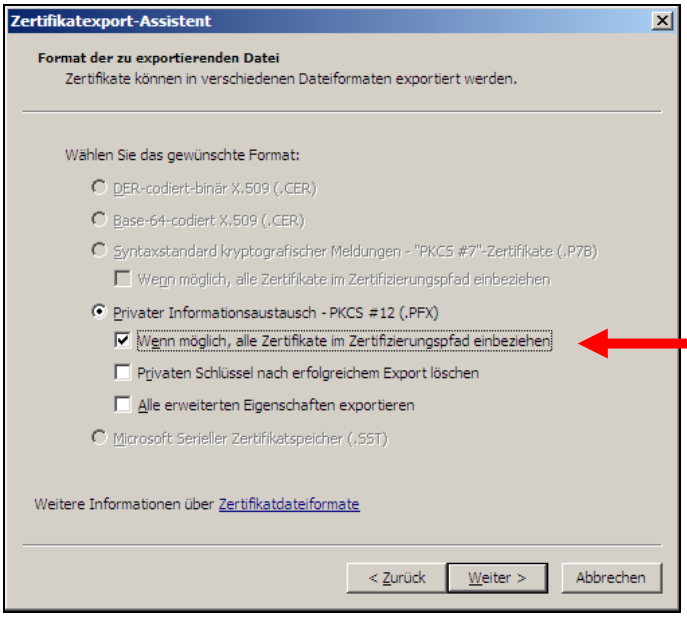
Wählen Sie: „**In Datei Kopieren**“, es öffnet sich der Zertifikatexport-Assistent, siehe Abbildung 19.

Abbildung 19:



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

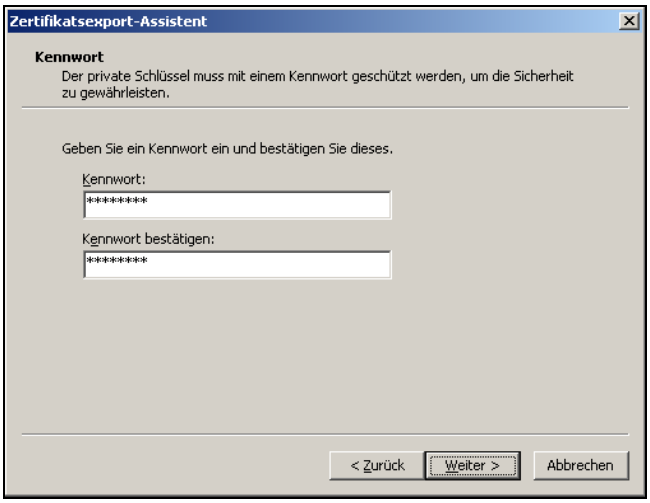
Abbildung 20:



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**.

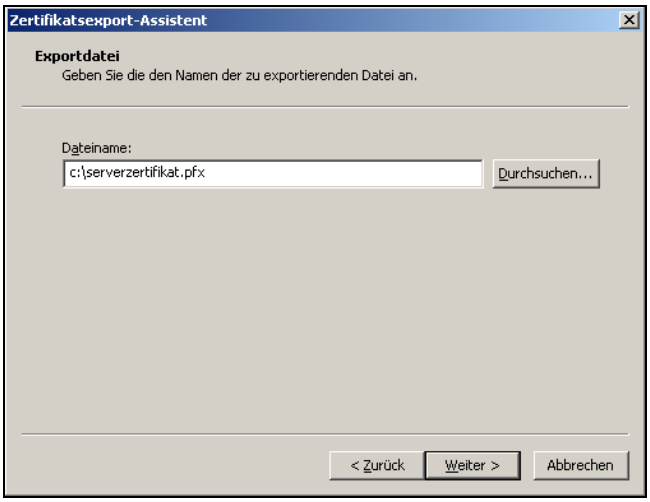
Abbildung 21:



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

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

Abbildung 22:



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**“.

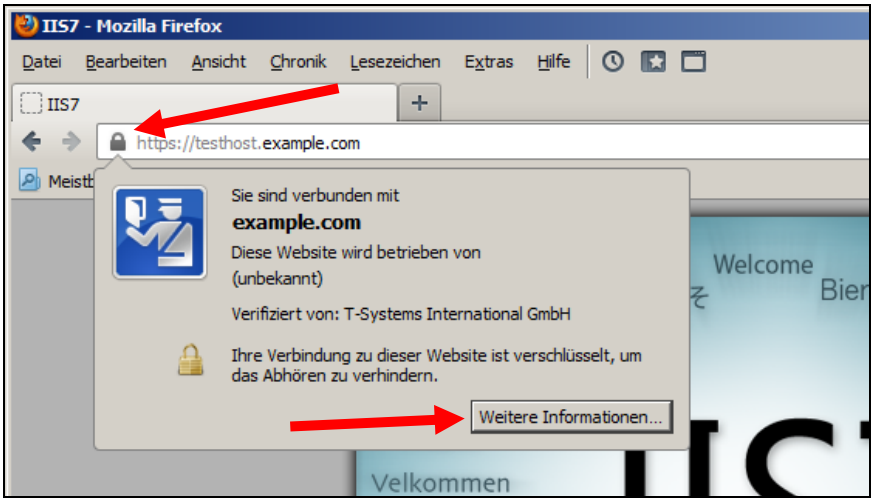
Der Vorgang ist hiermit abgeschlossen und Sie können den Servermanager nun beenden.

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. Andere Browser stellen den SSL-Modus ggf. anders dar. Exemplarisch ist hier die Darstellung im Firefox (Abbildung 23-25) sowie im Internet Explorer (Abbildung 26-29) aufgeführt.

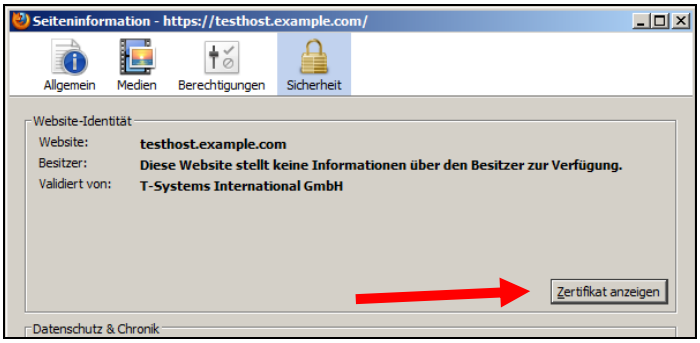
Firefox:

Abbildung 23 (Firefox 18):



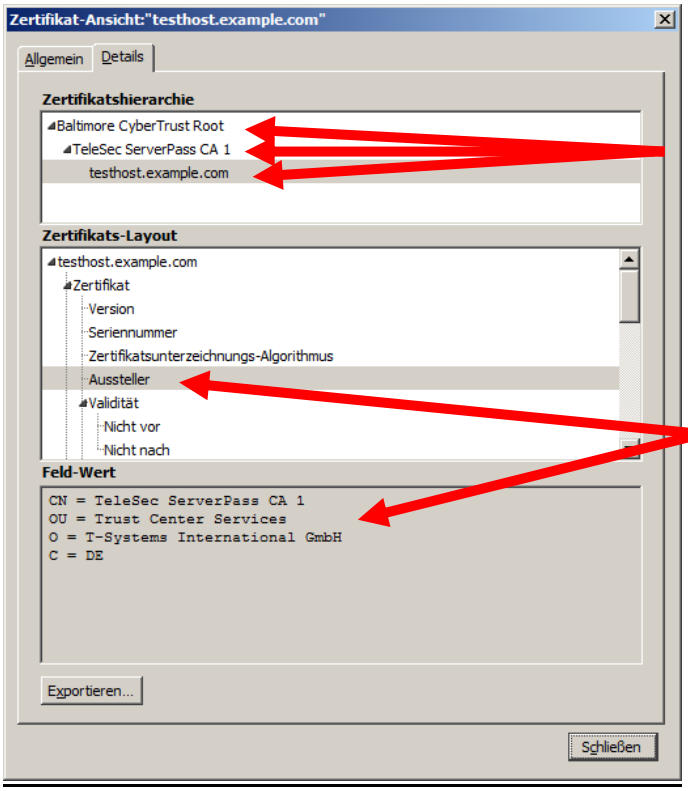
Beim Firefox lassen sich über einen Klick auf das Schloss Details zum verwendeten Zertifikat anzeigen.
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 24 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

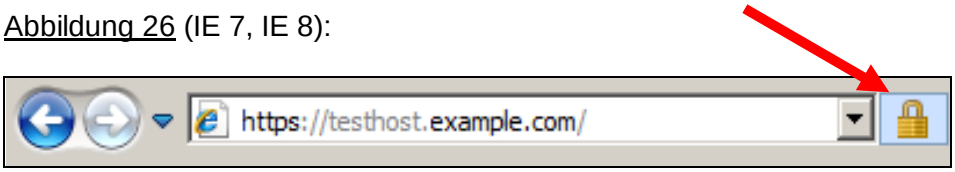
Abbildung 25 (Firefox 18):



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“

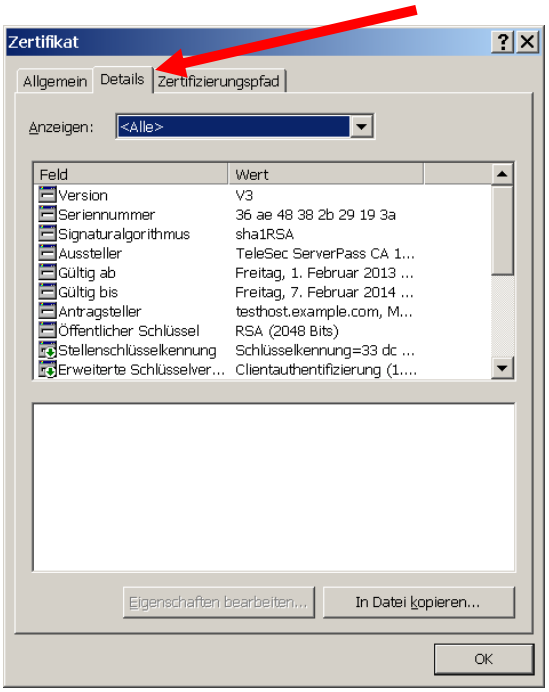
Internet Explorer

Abbildung 26 (IE 7, IE 8):



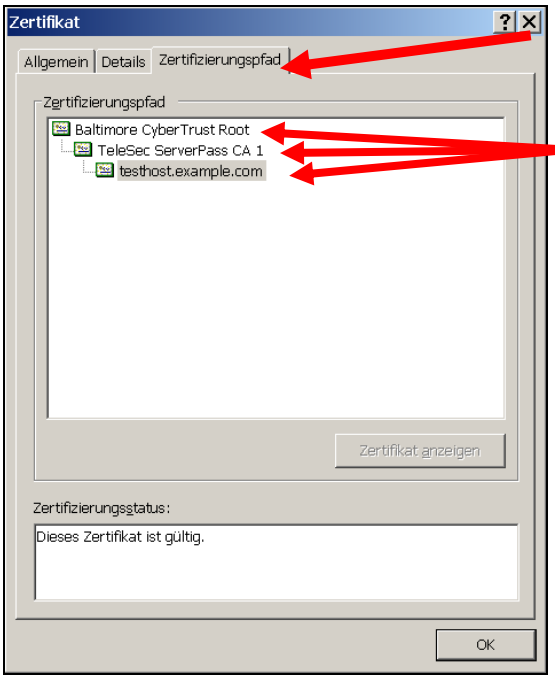
Beim Internet Explorer lassen sich die Zertifikatsdetails durch Doppelklick auf das Schloss anzeigen.
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 27.

Abbildung 27 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 28.

Abbildung 28 (Die Zertifikatskette)



Darstellung der kompletten Zertifikatskette

So wie in Abbildung 28 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“

https://www.telesec.de/serverpass -> Support -> Downloadbereich -> Anleitungen