TeleSec ServerPass

Zertifikatserneuerung mit dem MS IIS 6.0

Version: 1.3
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_6.doc		Requesterzeugung Microsoft IIS 6.0 Webserver

Version	Stand	Status
1.3	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
Zertifikatserneuerung mit dem MS IIS 6.0

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	12.01.2011	W. Bohn	Erster Entwurf
1.0	20.01.2011	W. Bohn	Inhalt- und Layoutanpassung
1.1	27.01.2011	W. Bohn	Inhalt- und Layoutanpassung
1.2	12.02.2013	W. Bohn	Inhaltliche Anpasung
1.3	10.04.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

1 Allgemeines

Dieses Dokument beschreibt die Requesterzeugung sowie die Einbindung der Zertifikate im Microsoft IIS 6.0 Webserver.

Der Ablauf im Microsoft IIS 5.0 verläuft ähnlich.

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 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 „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 Microsoft IIS 6.0 Webserver

Die Beschreibung bezieht sich auf folgende Softwarekonstellation:

Microsoft Internet Information Server 6.0, deutsch
Microsoft Server 2003 SP2, deutsch
Internet-Explorer 7 oder höher

Voraussetzung: Der Webserver läuft bereits im SSL-Modus

Der ursprüngliche Request des zu erneuerten Zertifikats kann nicht noch einmal verwendet werden!

Man muss gemäß dieser Anleitung einen „Erneuerungs-Request“ erzeugen.

Bitte beachten Sie hierzu auch die Angaben unter **Punkt 2.3.0** „Verwendung des privaten Schlüssel“.

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) V5.0 / V6.0“ → „Installation der CA-Zertifikate im IIS 5.0 u. IIS 6.0“

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.

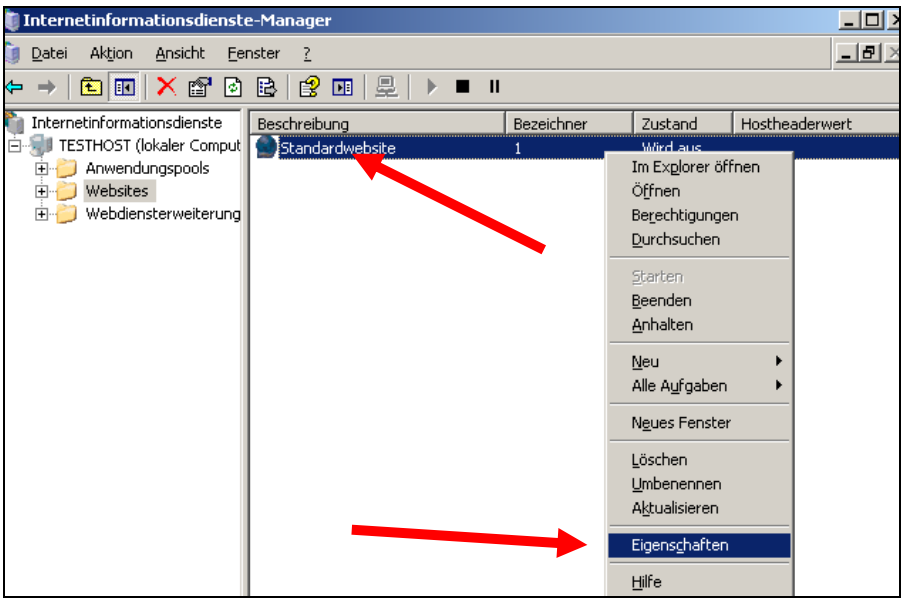
Achtung: eine nochmalige Verwendung eines bereits für eine Beauftragung verwendeten Server-Schlüssels ist nicht zulässig.
Daher ist ggf. die Erzeugung eines neuen Zertifikat-Requests erforderlich.
Folgen Sie hierzu bitte der Anleitung „Microsoft Internet Information Server (IIS) V6.0 Zertifikat-Requesterzeugung, Installation der Zertifikate“, Schritt 1.

2.2 Requesterzeugung

Zunächst öffnen Sie den Internetdienstemanager, siehe Abb.1. Diesen erreichen Sie über:

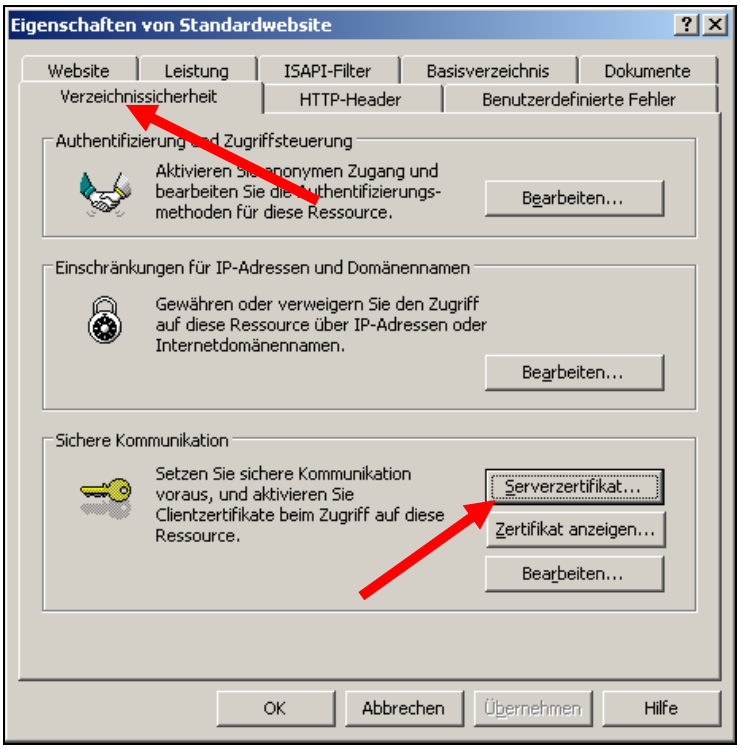
Start → Verwaltung → Internetdienstemanager

Abbildung 1:



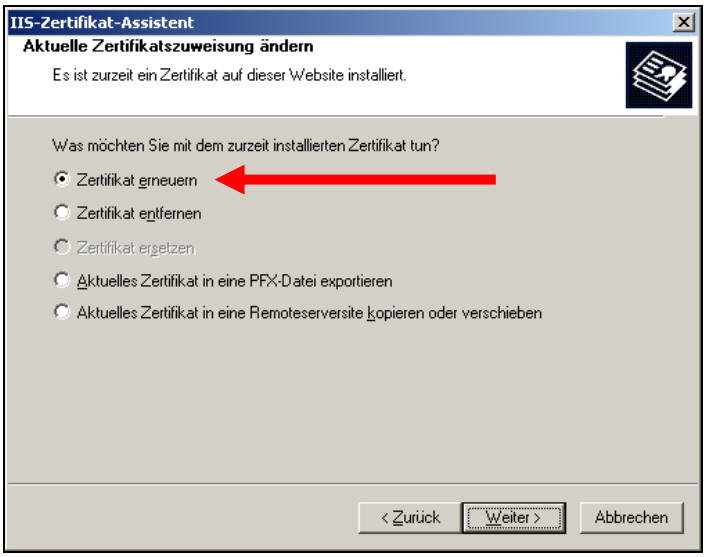
Markieren Sie die „**Standardwebseite“** mit der rechten Maustaste und wählen dann "**Eigenschaften**". Es erscheint Abbildung 2.

Abbildung 2

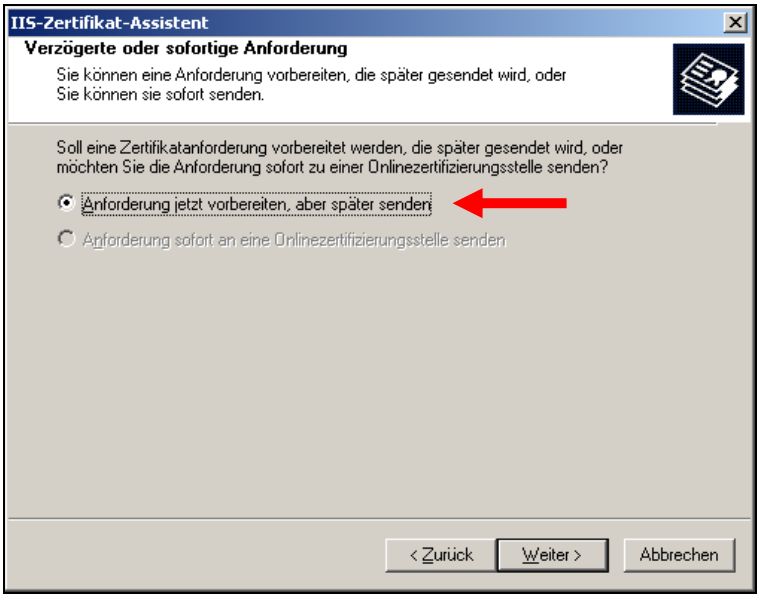


Wählen Sie den Karteireiter „**Verzeichnissicherheit**“ und dann unter „**Sichere Kommunikation**“ den Button „**Serverzertifikat...**“.
Daraufhin öffnet sich der IIS-Zertifikat-Assistent, siehe Abbildung 3.

Abbildung 3

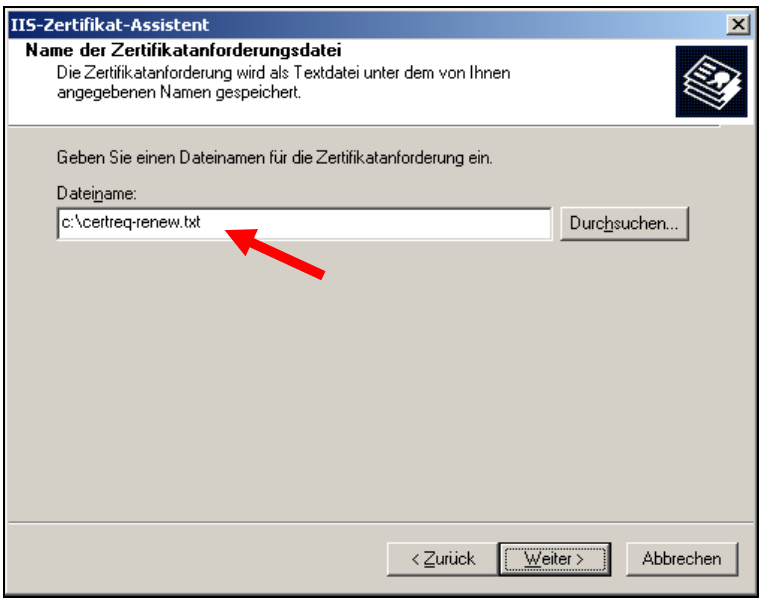


In Abbildung 3 wählen Sie die Option **„Zertifikat erneuern“.**
Abbildung 4



Wählen Sie die Option: „**Anforderung jetzt vorbereiten, aber später senden**“.

Abbildung 5



In Abbildung 5 legen Sie den Pfad für die Requestdatei fest.
Diese Datei enthält später den Zertifikatsrequest, z. B. „c:\certreq-renew.txt“

Abbildung 6

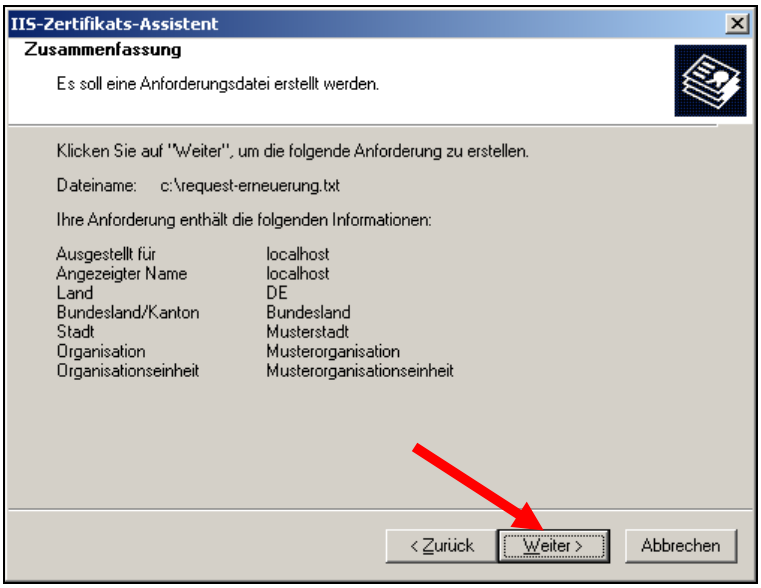
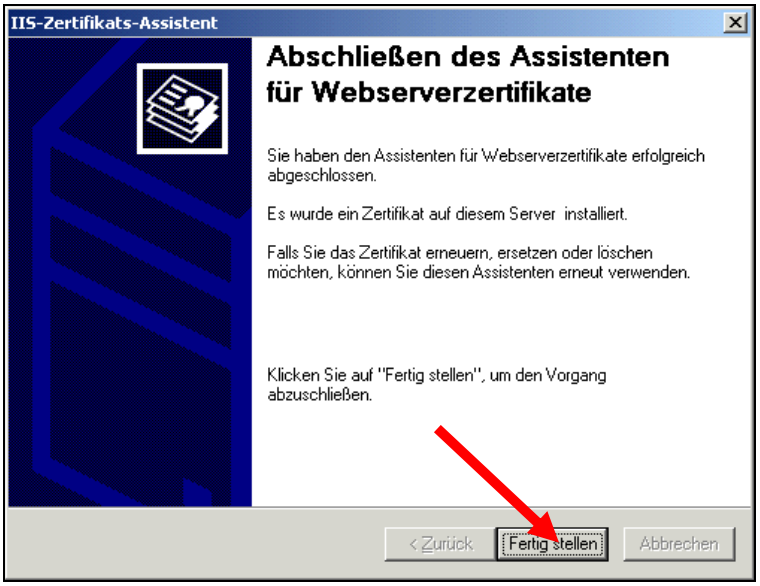


Abbildung 6 zeigt die Zertifikatinhalte des zu erneuernden Zertifikats.

Abbildung 7



Durch Klicken des Buttons „**Fertig stellen**“ wird die Requesterzeugung abgeschlossen.

Hierdurch erhalten Sie die Requestdatei „c:\certreq-renew.txt“, siehe Abbildung 8.

Der Request trägt die gleichen Angaben (Common Name, Organisation usw.) wie das zu erneuernde Zertifikat.

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 (certreq-renew.txt)

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

2.3 Beauftragung des Serverzertifikats

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

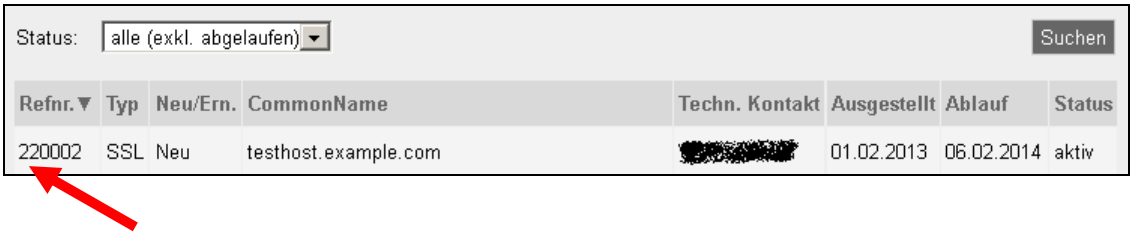
Unabhängig von der Restlaufzeit des zu erneuernden Zertifikats wird das neue Zertifikat sofort ausgestellt und steht i. d. R. sofort zum Download bereit.

Melden Sie sich am Kundenportal „myServerPass“ an.

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

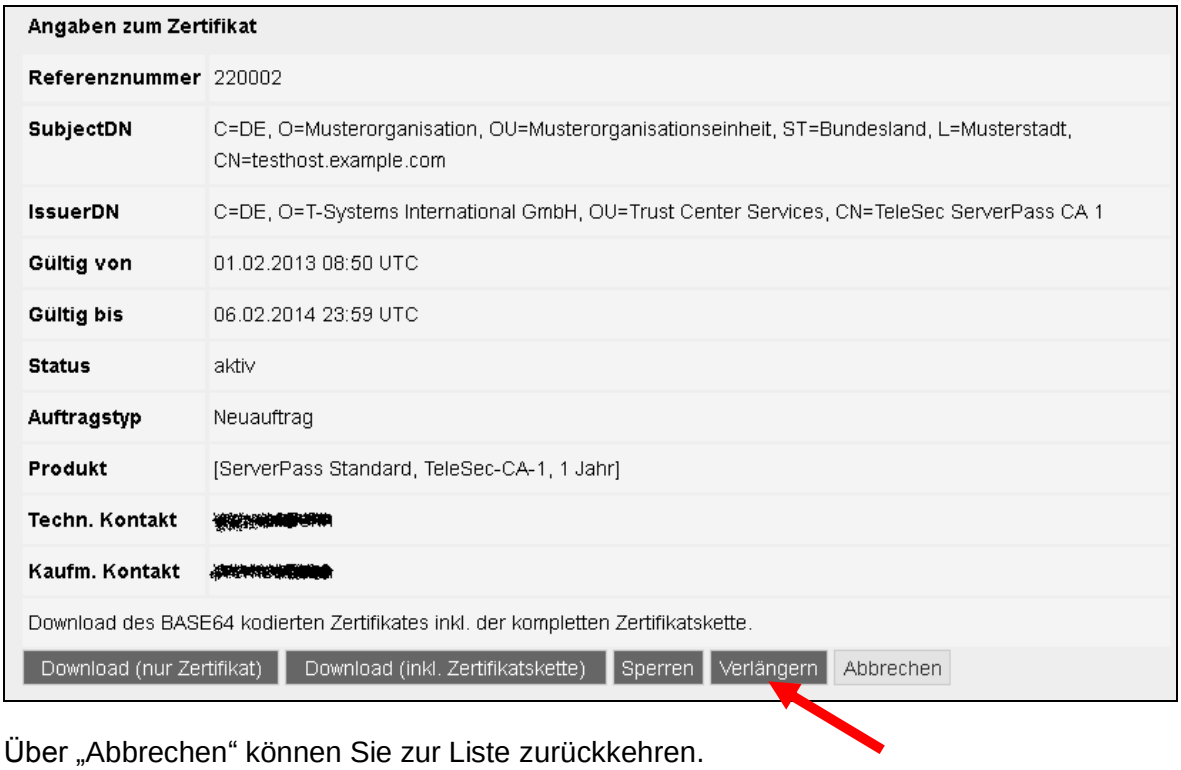
Unter dem Menüpunkt “Meine Zertifikate“ erscheint eine Liste aller Ihrer Zertifikate, siehe Abbildung 9.
Hier können Sie nun das zu erneuernde Zertifikat anhand der Referenznummer ermitteln. ggf. lassen sich die Zertifikatseinträge durch Klicken auf die „Referenznummer“ oder den „Common Name“ anzeigen.

Abbildung 9 (Ausschnitt des Kundenportals):



Durch Klicken auf die Referenznummer lassen sich die Zertifikatdetails anzeigen.

Abbildung 10



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 11.

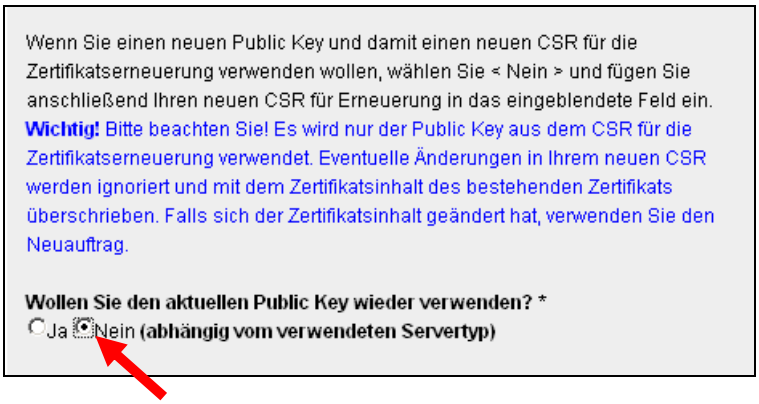
Abbildung 11:

Anschließend wird die Verwendung des Public Keys abgefragt, siehe Abbildung 12.

2.3.1 Die Verwendung des Public Keys bei der Erneuerung

Bei einer Erneuerung stehen zwei Optionen zur Auswahl, siehe Abbildung 12:

Abbildung 12 (Verwendung des Public Keys)



Im Auftragsformular werden alle Details des zu erneuernden Zertifikats angezeigt.

Public Key Wiederverwendung:
Wichtig: Hier wählen Sie die Option **nein** !
In das erscheinende Feld „" **Mein PKCS#10 Zertifikats-Request**" (inklusive der ---- BEGIN.... und ----END... Zeilen).

Nach dem Einfügen werden die Request-Inhalte zur Kontrolle angezeigt,
siehe Abbildung 13.

Abbildung 13

Prüfen Sie die angezeigten Zertifikatsdaten sowie Ihre Kontaktdaten und senden das Formular ab.
Das Auftragsformular für den Serverpass wird nach dem Absenden zum Abspeichern bzw. Ausdrucken angeboten. Alternativ können Sie sich das Formular per Email zuschicken lassen.
Bitte notieren Sie sich die Referenznummer des Auftrages.

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

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

2.4 Herunterladen und importieren des erneuerten Zertifikats

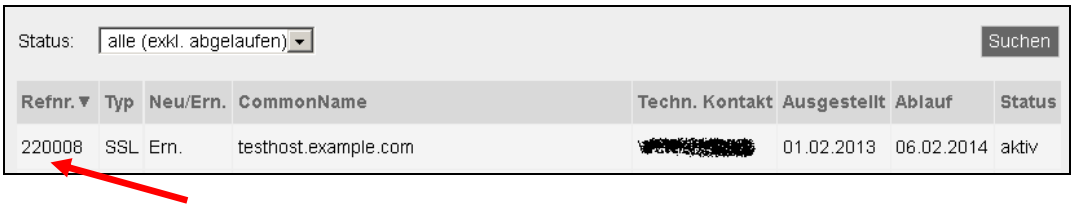
2.4.1 Herunterladen des erneuerten Zertifikats

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)

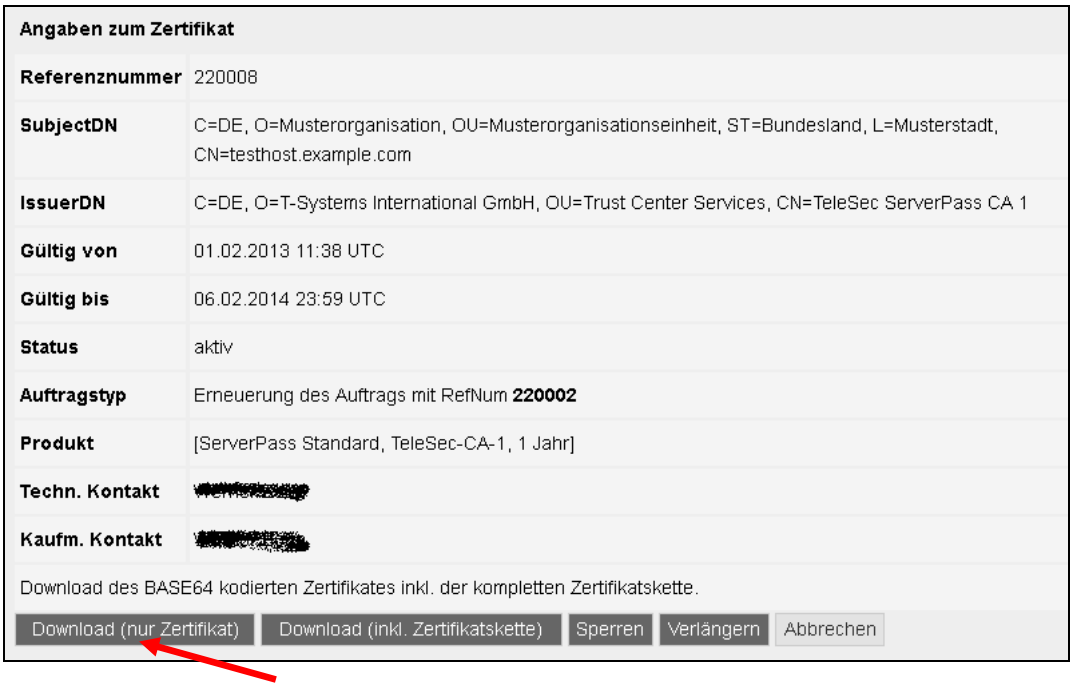
Wählen Sie den Menüpunkt „Meine Zertifikate“
Hier werden nun alle Ihre Zertifikate aufgelistet, siehe Abbildung 14.

Abbildung 14



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

Abbildung 15



Wie in Abbildung 15 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-234567.pem“ und sie liegt nun unter c:\.

Die herunter geladene Datei enthält das Server-Zertifikat, wie in Abbildung 16 dargestellt.

Abbildung 16 (servpass-234567.pem)

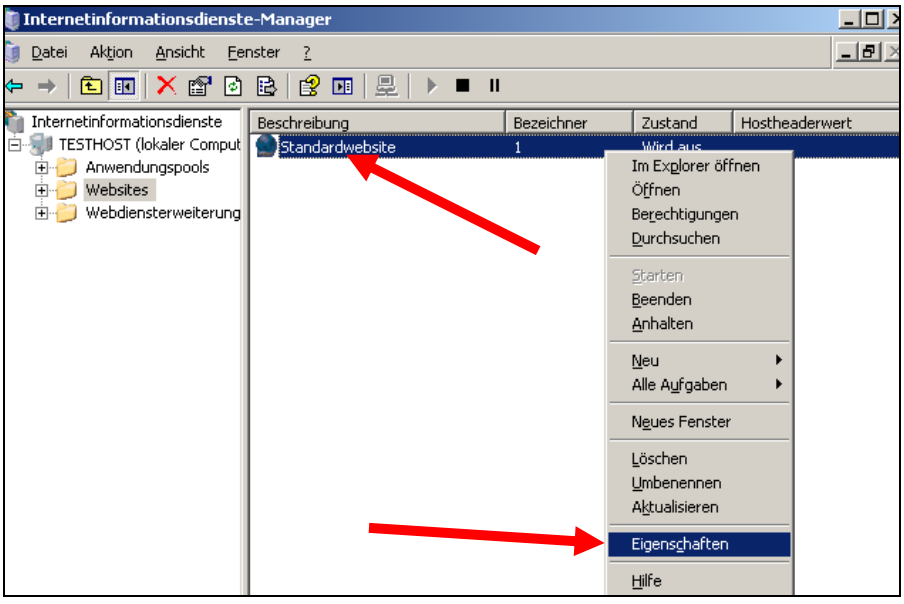
-----BEGIN CERTIFICATE-----
IUHILHJKGUTUGHJOILUOJHKLJLUOHJKHHLKKLHKKLHKLHKLU
JHKHKKJLJKHKJHJKHJK786765HJKHKJHJKHJKHJKHJKHJKJK
.....
KLMKLPZQW4onheuHZIIO5BugGDRDZ878GJHKFDRTSXY45dfdgfjj5677
-----END CERTIFIQATE -----

2.4.2 Import des Serverzertifikats

Öffnen Sie den Internetinformationsdienste-Manager, siehe Abbildung 17. Sie erreichen ihn über:

Start → Verwaltung → Internetdienste-Manager

Abbildung 17:



Markieren Sie die „**Standardwebseite“** mit der rechten Maustaste und wählen dann "**Eigenschaften**". Es erscheint Abbildung 18.

Abbildung 18

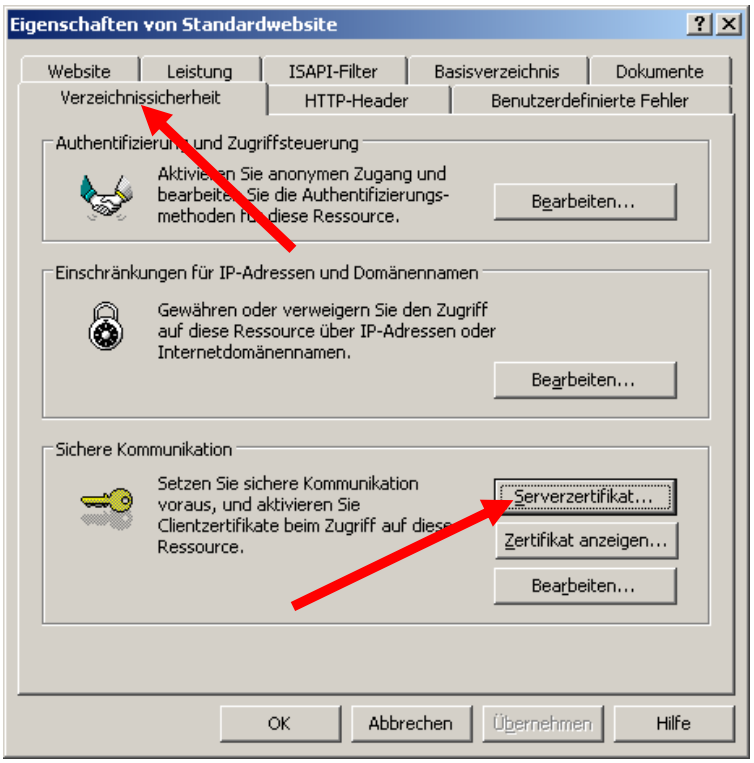
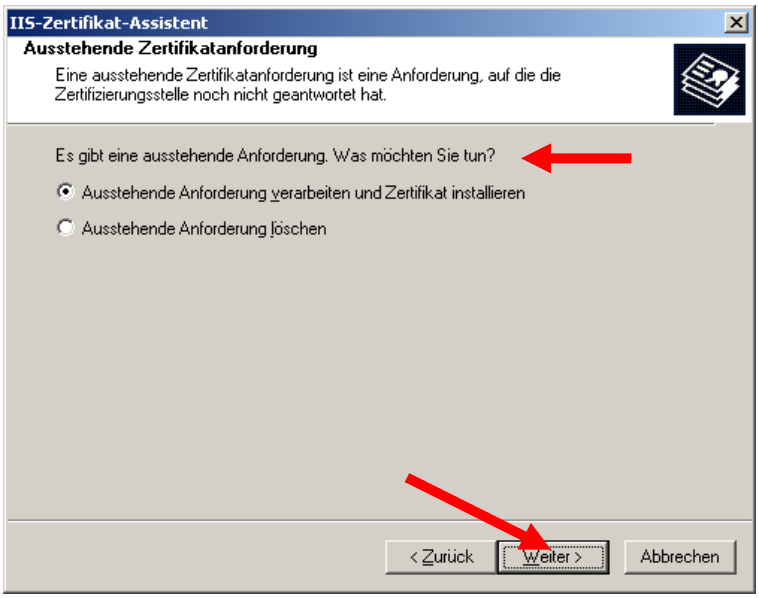
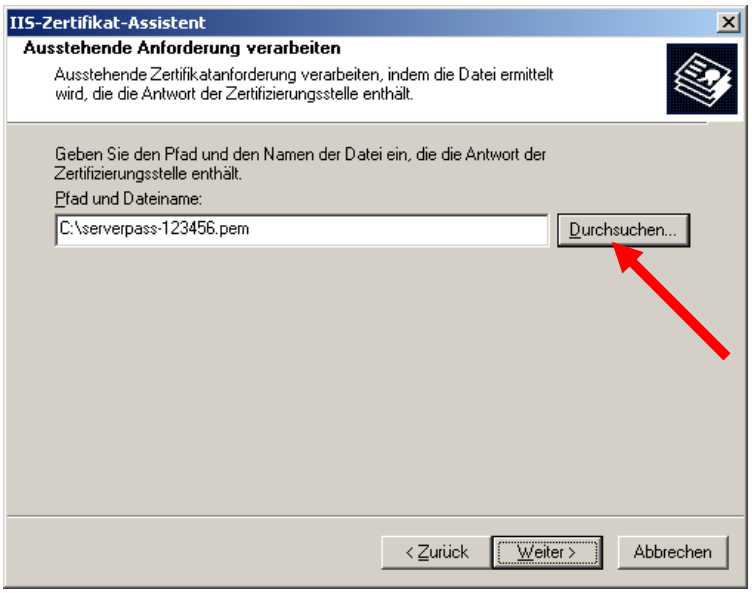


Abbildung 19



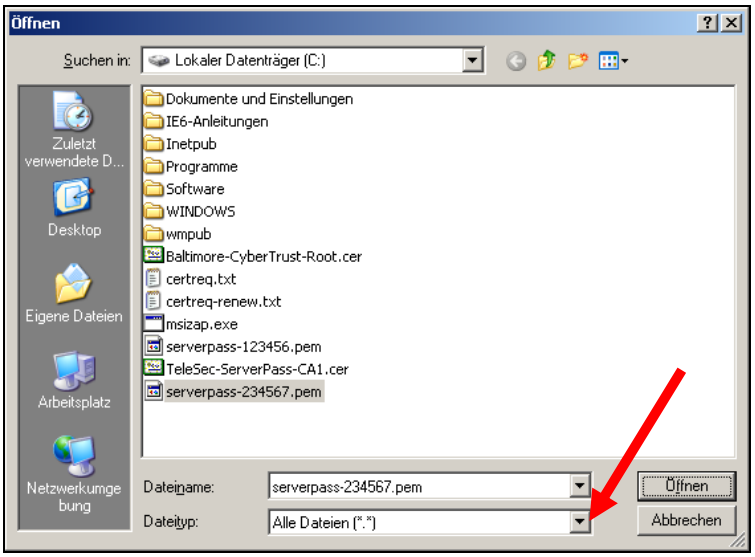
Wie in Abbildung 19 dargestellt, wählen Sie die Option:
„**Ausstehende Anforderung verarbeiten und Zertifikat installieren**“.

Abbildung 20



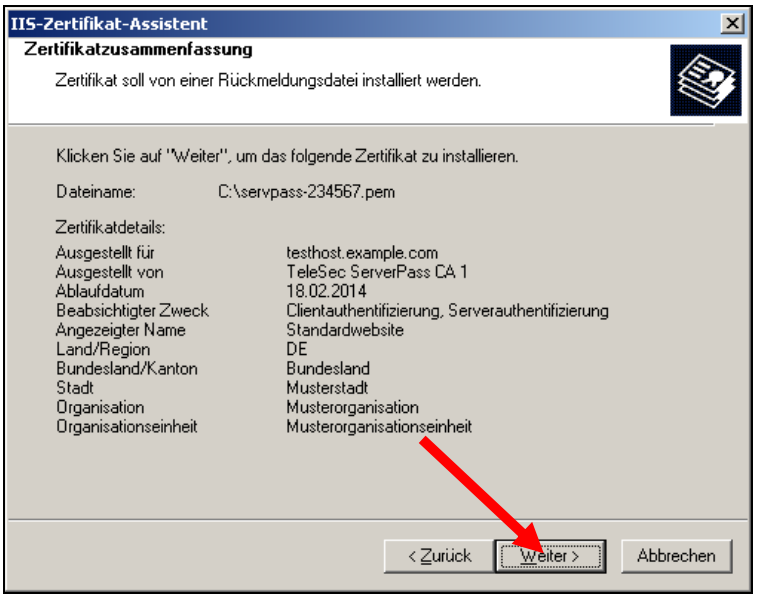
Wie in Abbildung 21 dargestellt, wird der Pfad zu der Zertifikatsdatei festgelegt.

Abbildung 21



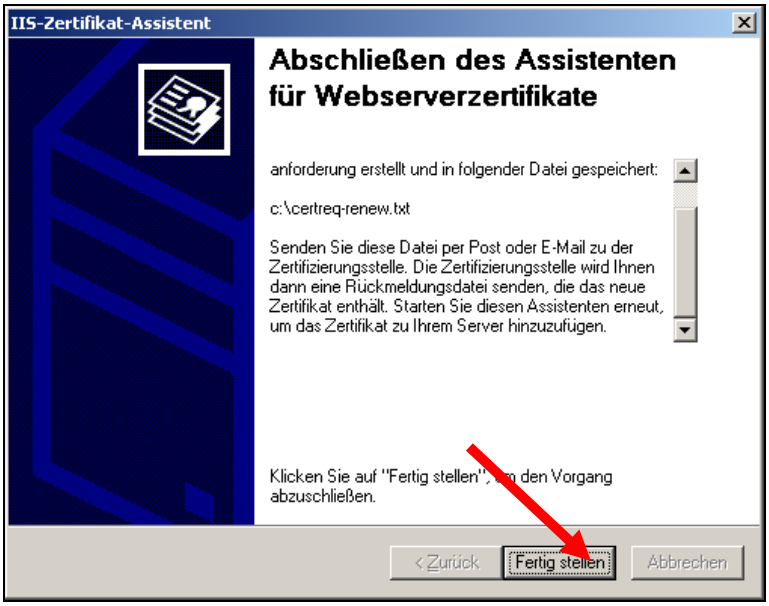
ggf. muss beim Import der Dateityp auf „Alle Dateien (*.*)“ gesetzt werden, siehe Abbildung 19.

Abbildung 20



Wie in Abbildung 20 dargestellt, werden alle Zertifikatsinhalte angezeigt.

Abbildung 21



Nachdem der Import durch klicken auf „Fertig stellen“ bestätigt wurde, ist die Installation des Serverzertifikates nun abgeschlossen.

In der Regel wird sofort das neue Zertifikat für die Verschlüsselung verwendet. ggf. ist jedoch ein Restart des Webservers erforderlich.

Es wird dringend empfohlen, den erzeugten Serverschlüssel zu sichern!

2.5 Sicherung des Serverschlüssels incl. Serverzertifikat

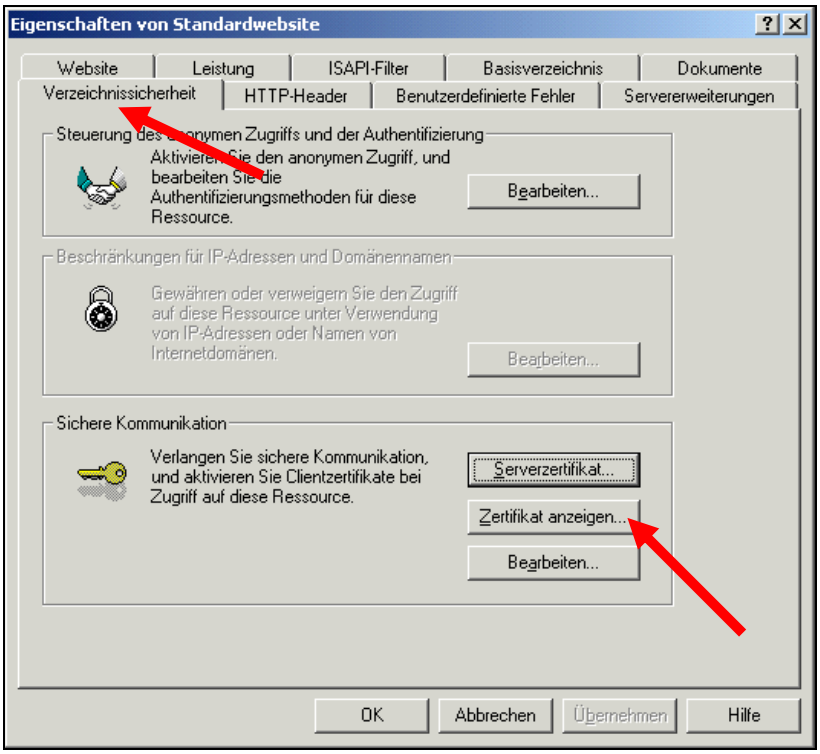
Nachfolgend wird die Sicherung aller Zertifikate incl. des privaten Schlüssels aufgezeigt.

Öffnen Sie erneut den Internet Informationsdienste-Manager:

Start → Verwaltung → Internetdienstemanager

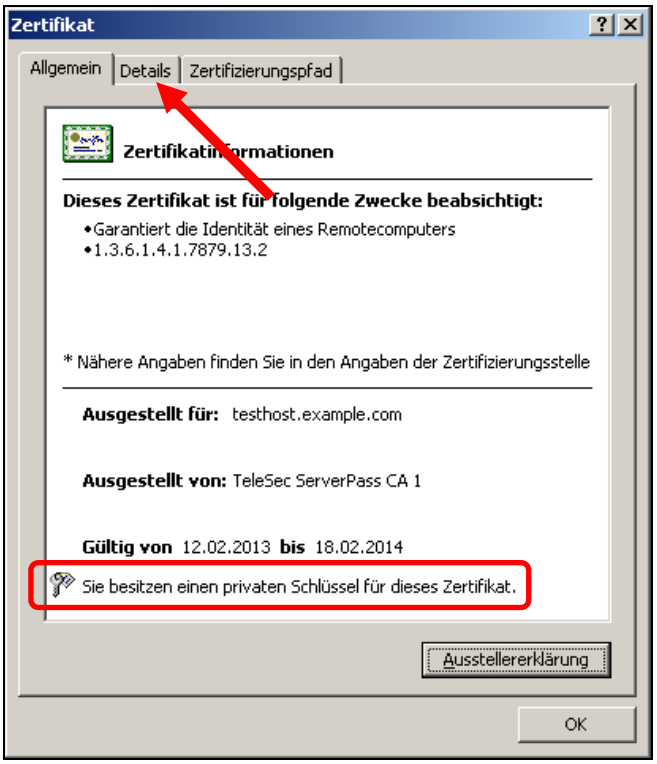
Markieren Sie die „**Standardwebseite“** mit der rechten Maustaste und wählen dann "**Eigenschaften**". Es erscheint Abbildung 22.

Abbildung 22



Hier wählen Sie den Reiter **Verzeichnissicherheit** und schließlich **Zertifikat anzeigen**, es erscheint Abbildung 23.

Abbildung 23

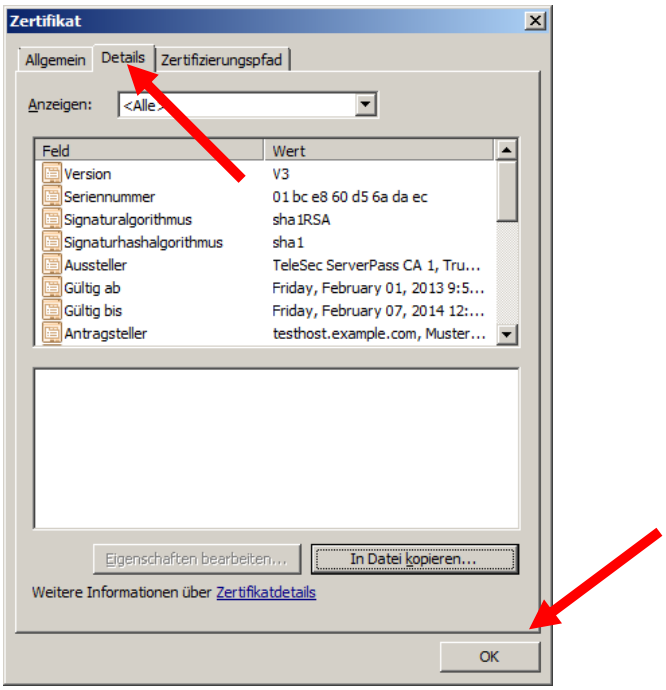


Achten Sie hier auf die korrekten Angaben für die Gültigkeit, „Ausgestellt für“ und „Aufgestellt von“.

Wichtig: Der Eintrag „**Sie besitzen einen privaten Schlüssel für dieses Zertifikat**“ muss erscheinen!

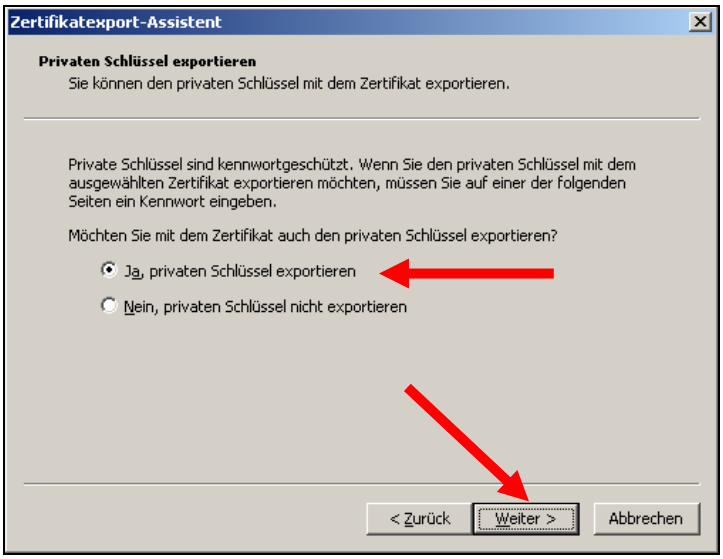
Anschließend wechseln Sie auf den Reiter **Details**, es erscheint Abbildung 24.

Abbildung 24



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

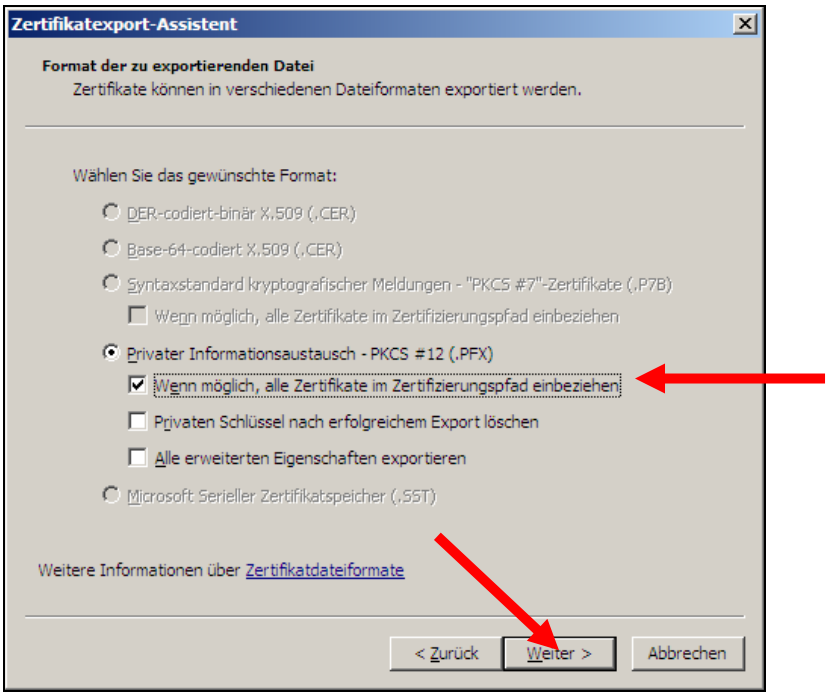
Abbildung 25:



Wichtig: Im Dialogfenster **Privaten Schlüssel exportieren** wählen Sie:
„Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?“

„Ja, privaten Schlüssel exportieren“

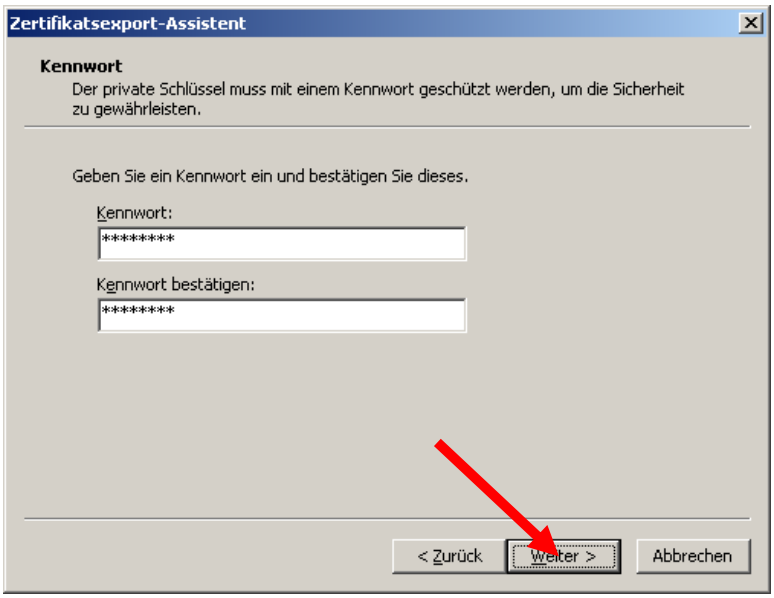
Abbildung 26:



Im Dialogfenster „Format der exportierenden Datei“ wählen Sie:
„Privater Informationsaustausch – PKCS #12 (.pfx)“

Und aktivieren lediglich die Option:
„Wenn möglich alle Zertifikate im Zertifizierungspfad einbeziehen.“

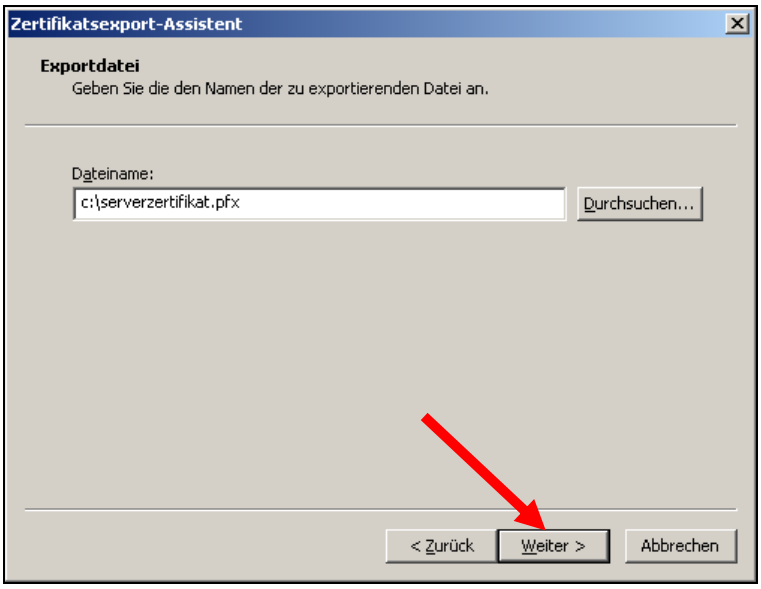
Abbildung 27



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.

Abbildung 29

Wie in Abbildung 29 dargestellt, wird der erfolgreiche Export bestätigt.

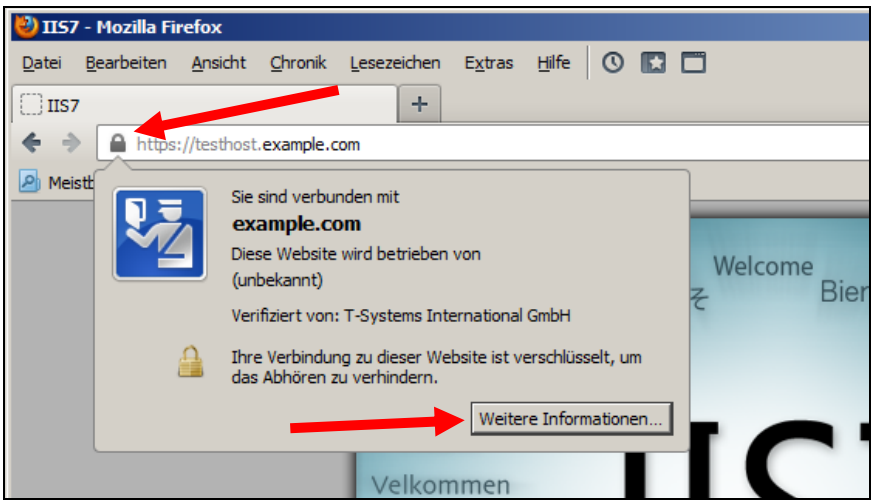
Der Vorgang ist hiermit abgeschlossen.

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 30-32) sowie im Internet Explorer (Abbildung 3335) aufgeführt.
Andere Browser stellen den SSL-Modus ggf. anders dar.

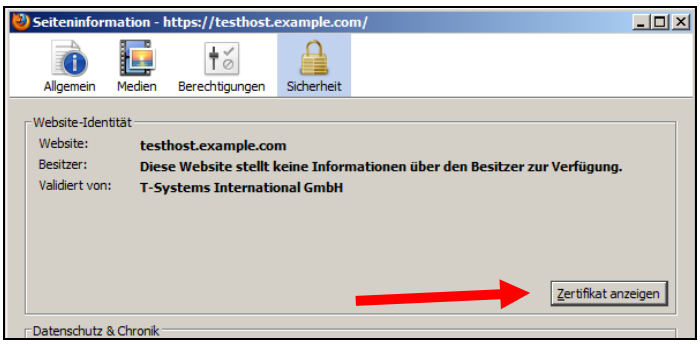
Firefox:

Abbildung 30 (Firefox 18):



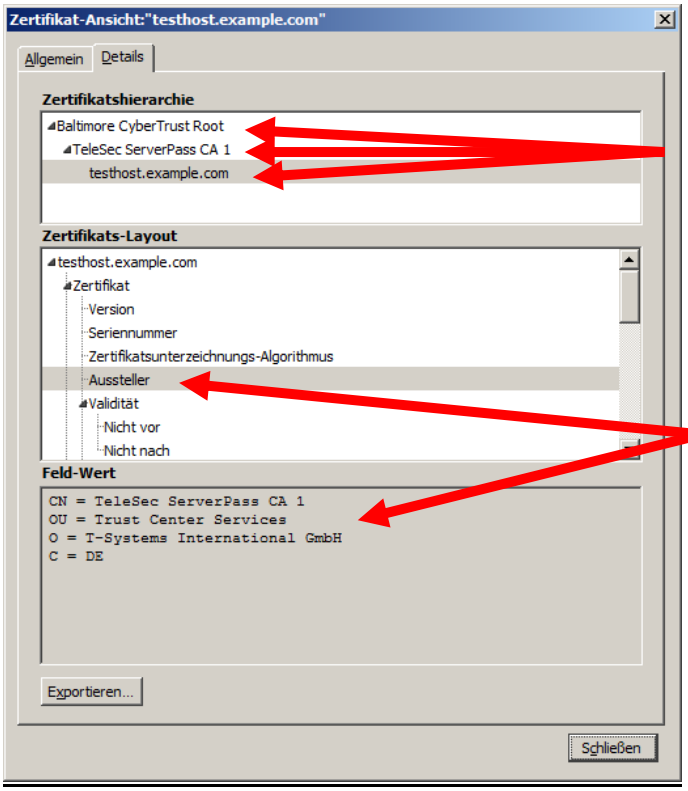
Beim Firefox lassen sich über einen Klick auf das Schloss Details zum verwendeten Zertifikat anzeigen.
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 31 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

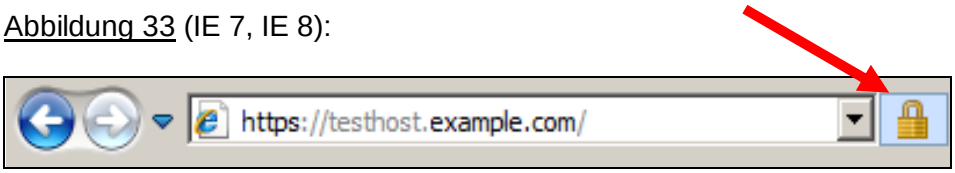
Abbildung 32 (Firefox 18):



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“

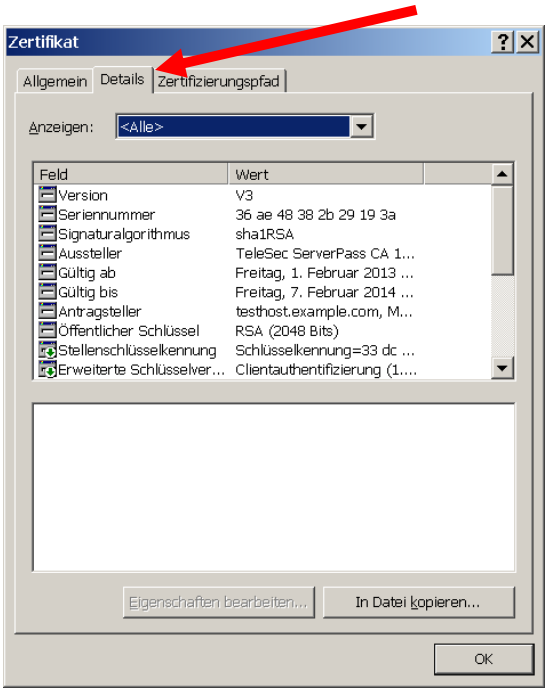
Internet Explorer

Abbildung 33 (IE 7, IE 8):



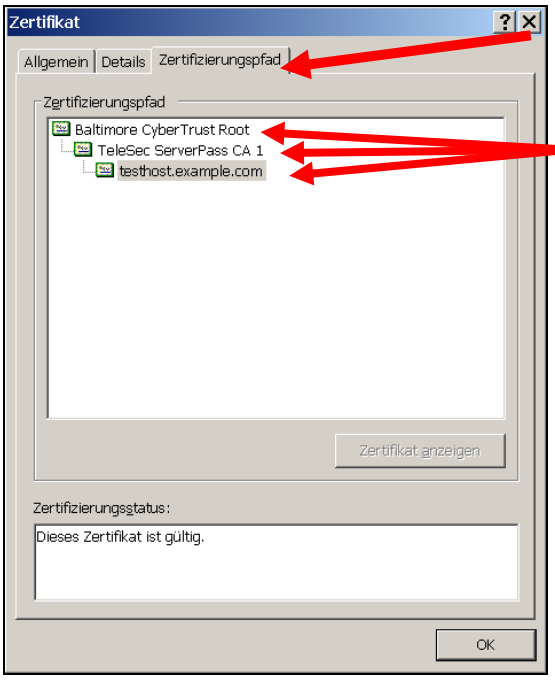
Beim Internet Explorer lassen sich die Zertifikatsdetails durch Doppelklick auf das Schloss anzeigen.
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 34.

Abbildung 34 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 35.

Abbildung 35 (Die Zertifikatskette)



Darstellung der kompletten Zertifikatskette

So wie in Abbildung 35 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.