

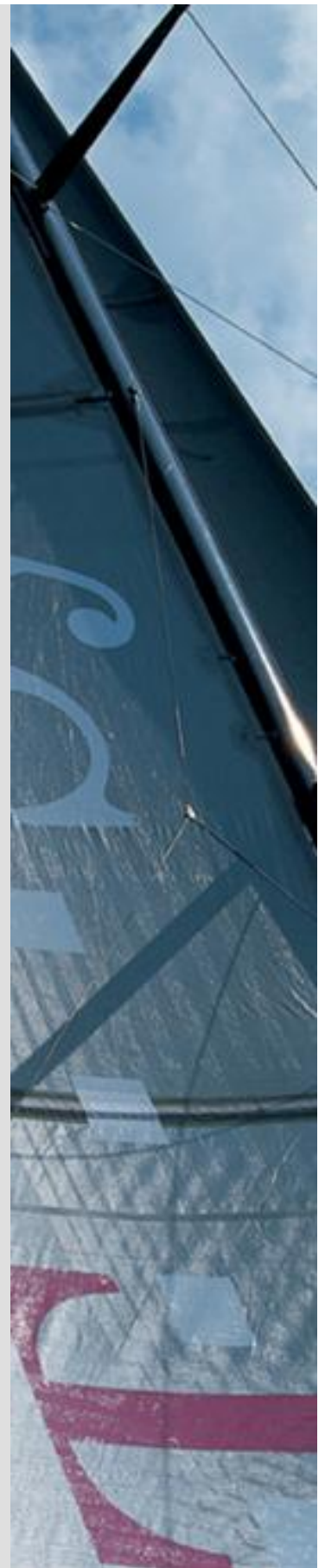
TeleSec ServerPass

Zertifikats-Requesterzeugung 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_req_inst_msiiis_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

Zertifikats-Requesterzeugung mit dem MS IIS 6.0

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	05.01.2011	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 Anpassung
1.3	10.04.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

1	Allgemeines	5
1.1	Testzertifikate.....	6
1.2	Spezielle Hinweise für Microsoft IIS 6.0 Webserver.....	7
2	Requesterzeugung, Beauftragung, Installation, Sicherung des privaten Schlüssels	8
2.1	Requesterzeugung.....	9
2.1.1	(*) Stichwort „Common Name“.....	13
2.2	Beauftragung des Serverzertifikats.....	16
2.3	Herunterladen und Import des Server-Zertifikats.....	17
2.3.1	Herunterladen des Server-Zertifikats.....	18
2.3.2	Import des Serverzertifikats.....	19
2.4	Sicherung des Serverschlüssels incl. Serverzertifikat.....	22
3	Kontrolle	27

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.

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

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 (**Certificate Practice Statement**) aufgeführten Hinweise. Insbesondere den erlaubten Zeichensatz.
Siehe hierzu: <https://www.telesec.de/serverpass/support/downloadbereich/category/20-certification-practice-statement-cps>

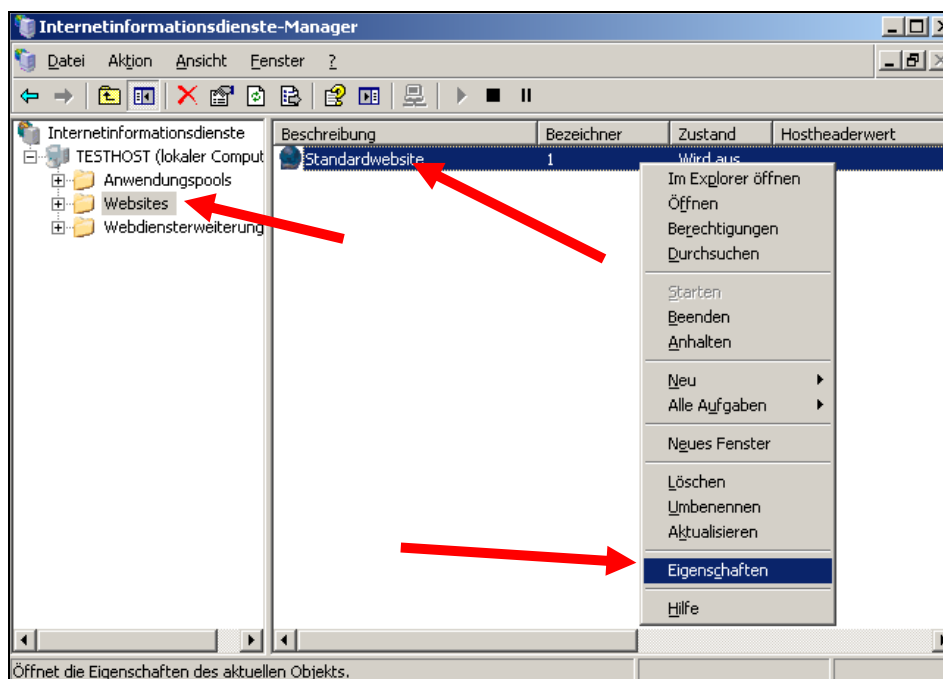
Vermeiden Sie die Verwendung von Feldern, die lediglich ein Leerzeichen enthalten!

2.1 Requesterzeugung

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

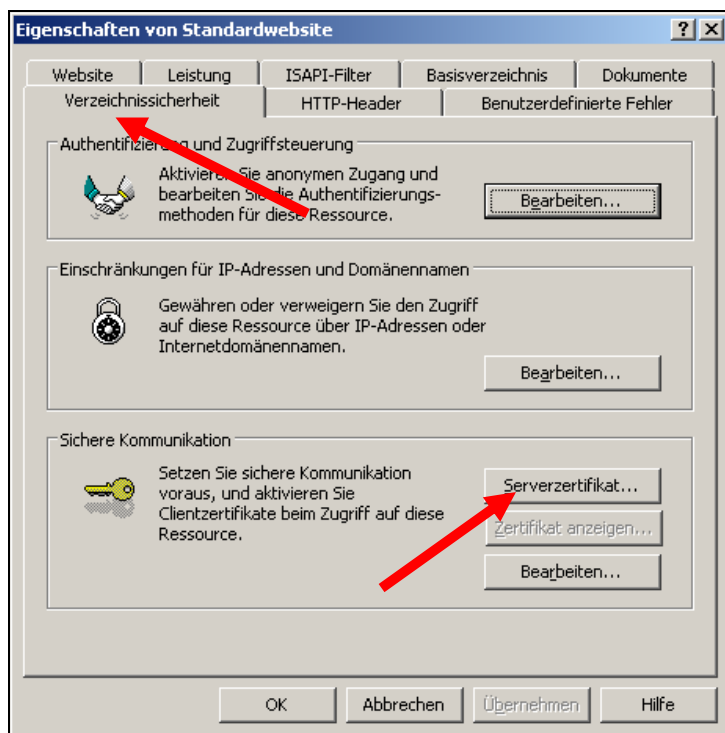
Start → Verwaltung → Internetdienstemanager

Abbildung 1:



Markieren Sie „**Websites**“ und anschließend die abzusichernde Webseite. Im Beispiel ist dies die „**Standardwebsite**“. Markieren Sie diese mit der rechten Maustaste und wählen dann "**Eigenschaften**". Es erscheint Abbildung 2.

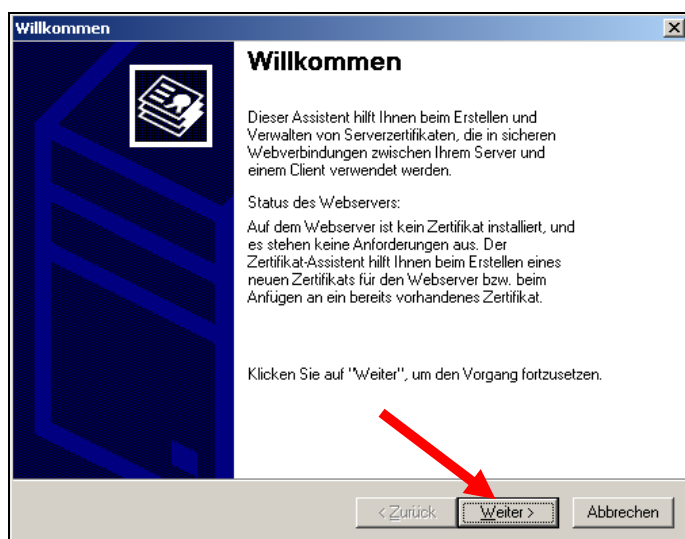
Abbildung 2



Wählen Sie den Karteireiter „**Verzeichnissicherheit**“ und dann unter „**Sichere Kommunikation**“ den Button „**Serverzertifikat...**“.

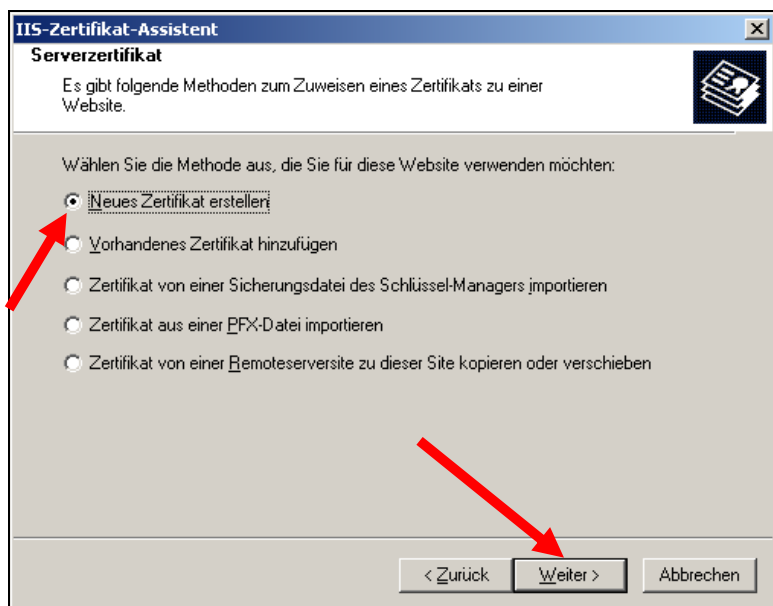
Daraufhin öffnet sich der IIS-Zertifikats-Assistent, siehe Abbildung 3.

Abbildung 3



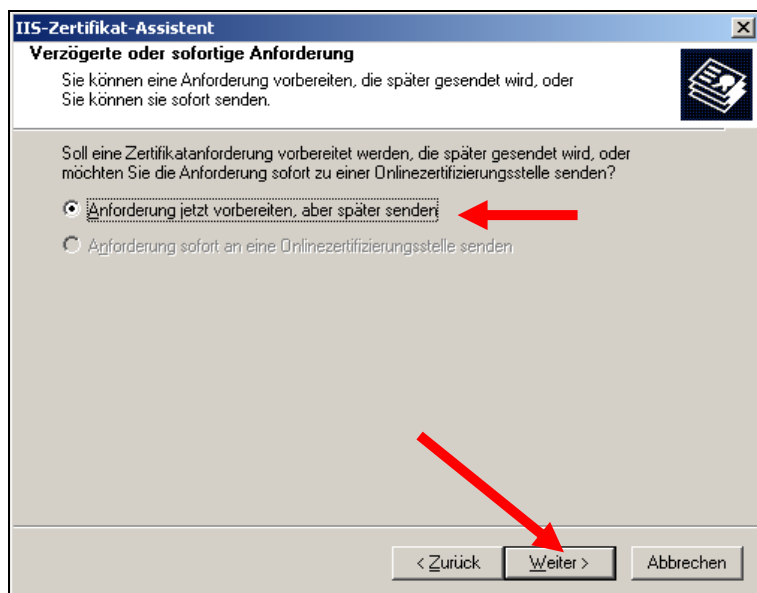
Es erfolgt eine kurze Erläuterung der Funktionen des Zertifikat-Assistenten.

Abbildung 4



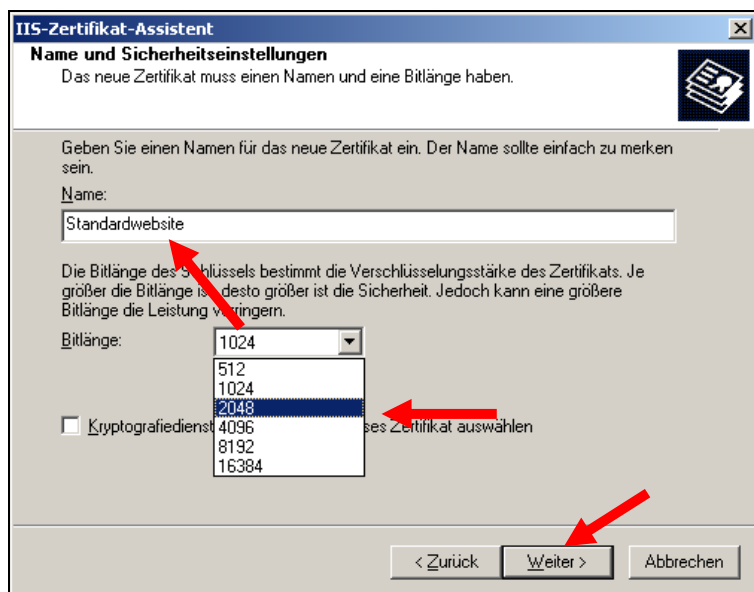
In Abbildung 4 wählen Sie die Option „**Neues Zertifikat erstellen**“.

Abbildung 5



In Abbildung 5 wählen Sie die Option:
„**Anforderung jetzt vorbereiten, aber später senden**“.

Abbildung 6



In Abbildung 6 wird neben einem Zertifikatsnamen auch die Festlegung der Bitlänge (Schlüssellänge) des zu erzeugenden Schlüssels verlangt. Je nach verwendeter Version des IIS können mehrere Bitlängen ausgewählt werden.

Empfohlen wird eine Bitlänge von 2048, maximal jedoch 4096 Bit.

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

Das Häkchen für SGC (Server Gated Cryptography) wird nicht gesetzt.

In den nun folgenden Fenstern tragen Sie die Angaben entsprechend Ihrer Vorgaben ein und schließen die Requesterzeugung ab, siehe Abbildung 7 bis 12.

Abbildung 7

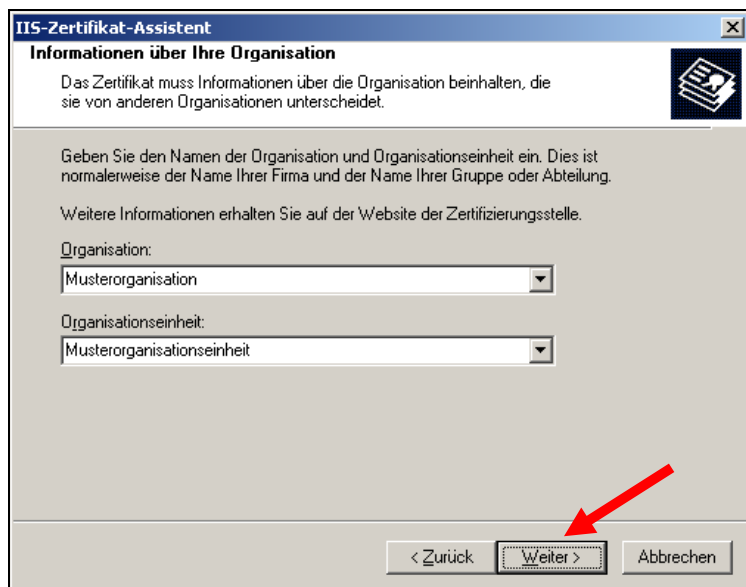
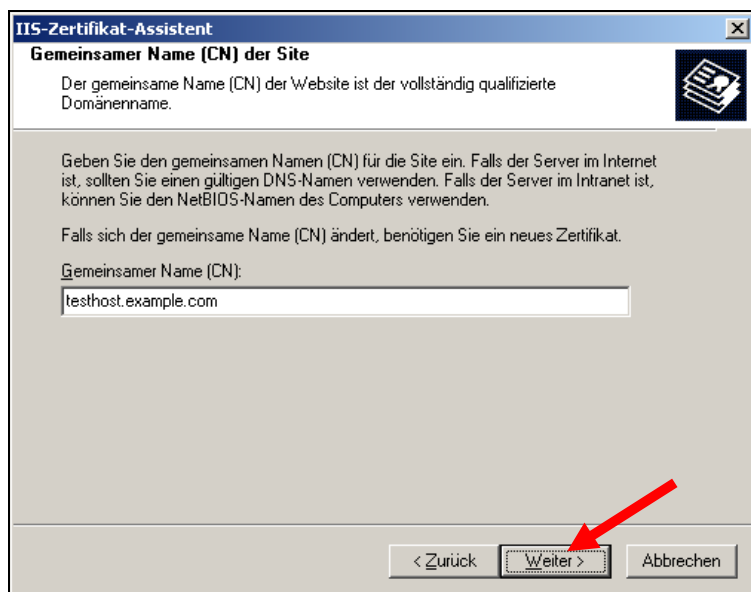


Abbildung 8 (Festlegung des Common Name *)



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).

Abbildung 9

IIS-Zertifikat-Assistent

Geographische Informationen

Die Zertifizierungsstelle benötigt folgende geographische Informationen:

Land/Region:

Bundesland/Kanton:

Ort:

Bundesland/Kanton und Ort müssen vollständige und offizielle Bezeichnungen sein und dürfen keine Abkürzung enthalten.

< Zurück **Weiter >** Abbrechen

Abbildung 10

IIS-Zertifikat-Assistent

Name der Zertifikatanforderungsdatei

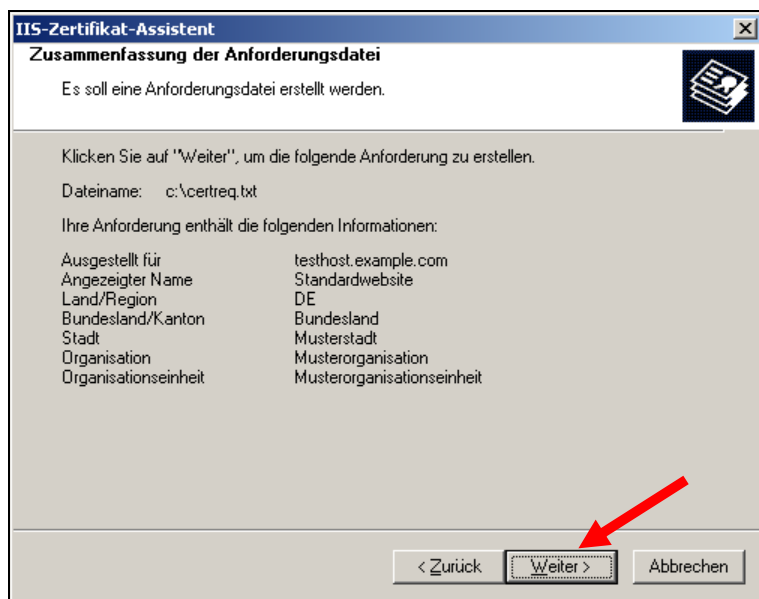
Die Zertifikatanforderung wird als eine Textdatei unter dem von Ihnen angegebenen Namen gespeichert.

Geben Sie einen Dateinamen für die Zertifikatanforderung ein.

Dateiname:

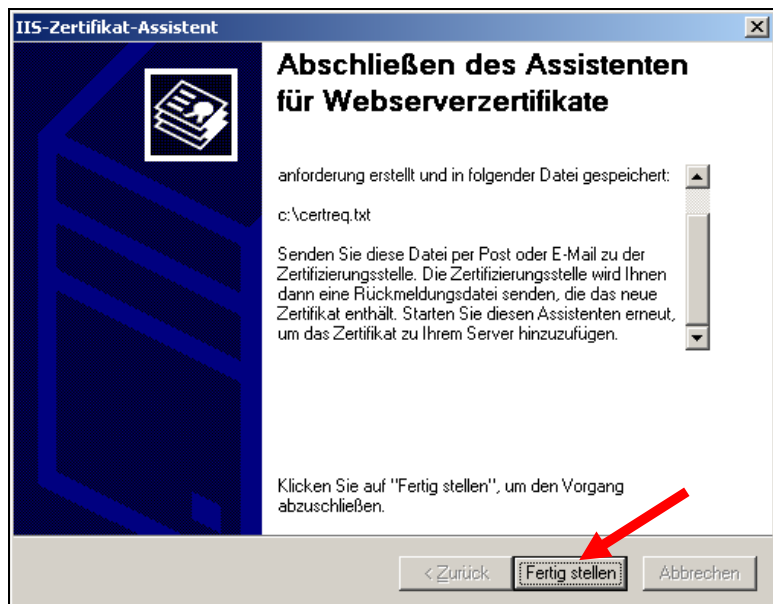
< Zurück **Weiter >** Abbrechen

Abbildung 11



Der Zertifikat-Assistent zeigt die Einträge an, die später im Zertifikat erscheinen. Kontrollieren Sie diese und führen den Vorgang weiter.

Abbildung 12



Durch Klicken des Buttons „**Fertig stellen**“ 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 13 angegeben.

Abbildung 13 (certreq.txt)

```

---BEGIN NEW CERTIFICATE REQUEST---
IUHILHJKGUTUGHJOILUOJHKLJLUOHJKHHLKKLHKLHKLHKL
JHKHKKJLJKHKJHJKHJK786765HJKHKJHJKHJKHJKHJKHJK
.....
KLMKLPZQW4onheuHZIO5BugGDRDZ878GJHKFDRTSXY45dfdgfjj5677
---END NEW CERTIFICATE REQUEST---

```

2.2 Beauftragung des Serverzertifikats

Nachdem der Request erzeugt wurde, können Sie auf unserer Internetseite einen Server-Pass bzw. einen ServerPassTest beauftragen.

<http://www.telesec.de/serverpass/index.html> (→ myServerPass)

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.

Füllen Sie das Online-Formular entsprechend Ihrer Vorgaben aus.

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 13 inklusive der ---BEGIN.... und ---END... Zeilen per cut & paste.

Nach dem Einfügen werden die Request-Inhalte zur Kontrolle angezeigt, siehe Abbildung 14.

Abbildung 14



Füllen Sie alle Kontaktfelder sowie alle Felder zur Auftragsprüfung entsprechen Ihrer Vorgaben aus und senden den Online-Auftrag 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.

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 mit den für den Download benötigten Angaben.

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.

www.telesec.de → ServerPass → Support → 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.

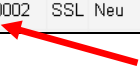
Wählen Sie das herunterzuladende Zertifikat durch Klick auf die Referenznummer aus, siehe Abbildung 15.

Abbildung 15:

Zum Sortieren der Übersicht klicken Sie bitte in die jeweilige Spaltenüberschrift.

Status:

Refnr.▼	Typ	Neu/Ern.	CommonName	Techn. Kontakt	Ausgestellt	Ablauf	Status
220002	SSL	Neu	testhost.example.com	[REDACTED]	01.02.2013	06.02.2014	aktiv



Es werden zwei Download-Formate angeboten, siehe auch Abbildung 16:

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

Abbildung 16

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


Auftragstyp Neuauftrag

Produkt [ServerPass Standard, TeleSec-CA-1, 1 Jahr]

Techn. Kontakt [REDACTED]

Kaufm. Kontakt [REDACTED]

Download des BASE64 kodierten Zertifikates inkl. der kompletten 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 17 dargestellt.

Abbildung 17 (servpass-123456.pem)

```

-----BEGIN CERTIFICATE-----
IUHILHJKGUTUGHJOILUOJHKLJLUOHJKHHLKKLHKKLHKLHKL
U
JHKHKKJLJKHKJHJKHJK786765HJKHKJHJKHJKHJKHJKHJKHJ
KJK
.....
KLMKLPZQW4onheuHZIIO5BugGDRDZ878GJHKFDRTSXY45dfd
gfjj5677
-----END CERTIFIQATE -----

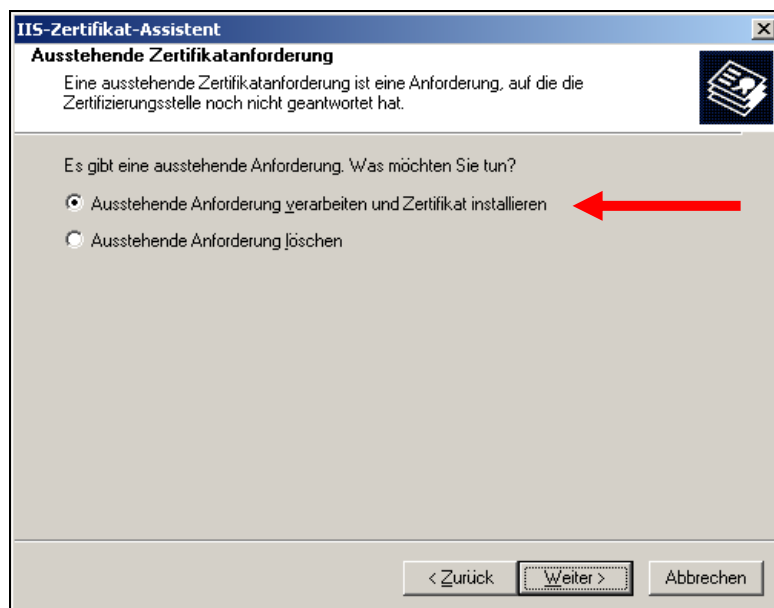
```

2.3.2 Import des Serverzertifikats

Für die Installation des Serverzertifikats rufen Sie erneut die Eigenschaften der Standardwebseite auf. Dann den Reiter **Verzeichnissicherheit** und schließlich **Serverzertifikat**, siehe Abbildung 2.

Anschließend öffnet sich der IIS-Zertifikat-Assistent, siehe Abbildung 18.

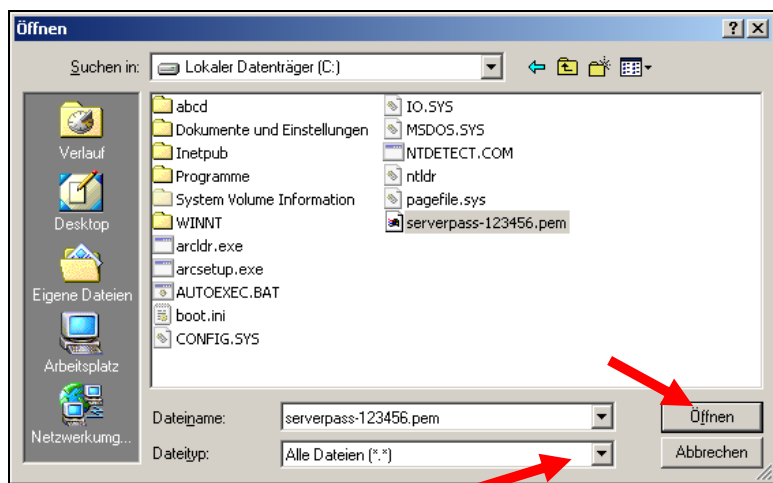
Abbildung 18



Wählen Sie die Option:

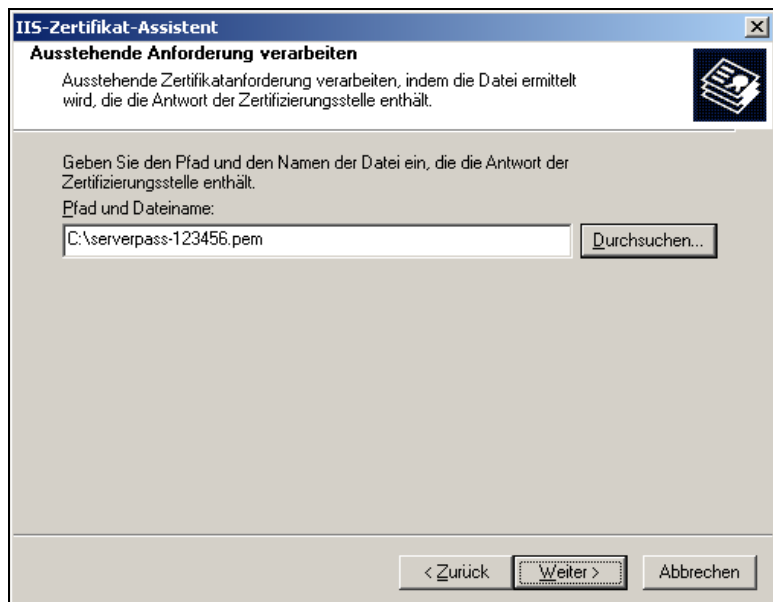
„**Ausstehende Anforderung verarbeiten und Zertifikat installieren**“.

Abbildung 19



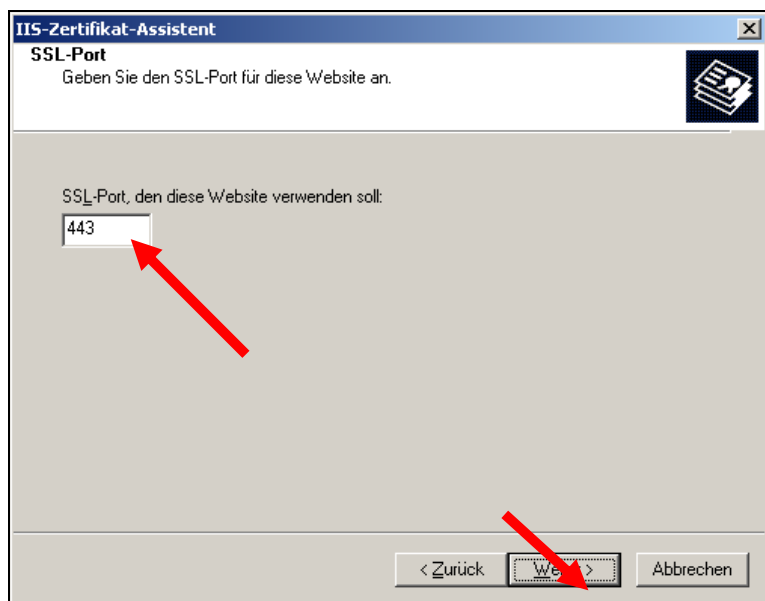
Wie in Abbildung 19 dargestellt, wählen Sie die Zertifikatsdatei aus, ggf. muss der Dateityp eingestellt werden auf „**Alle Dateien (*.*)**“.

Abbildung 20



Folgen Sie dem Assistenten durch Klicken auf „**Weiter**“, es erscheint Abbildung 21.

Abbildung 21



In Abbildung 22 wird der zu verwendete Port für die SSL-Verbindung abgefragt. Standardmäßig wird der SSL-Port **443** verwendet.

Abbildung 22

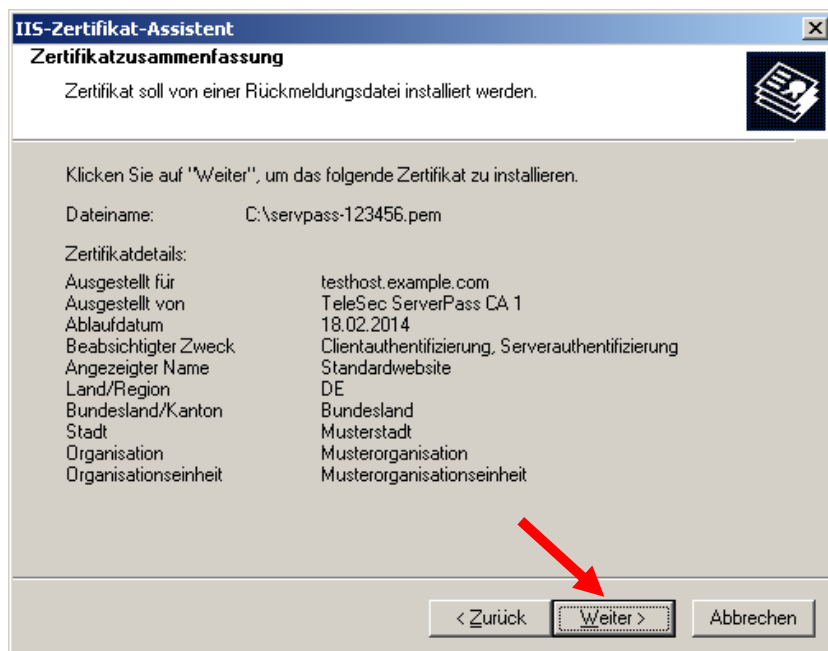


Abbildung 22 listet alle relevanten Daten des zu importierenden Zertifikats auf.

Folgen Sie dem Zertifikats-Assistenten bis zum Ende des Imports.

Nachdem der Webserver neu gestartet wurde, können verschlüsselte Verbindungen aufgebaut werden.

Es wird dringend empfohlen, den erzeugten Serverschlüssel zu sichern.

2.4 Sicherung des Serverschlüssels incl. Serverzertifikat

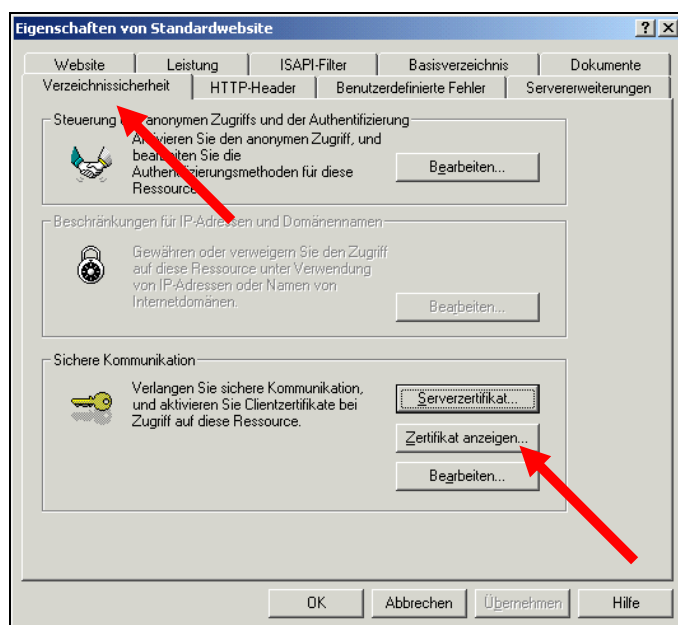
Nachfolgend wird die Sicherung aller Zertifikate incl. des privaten Schlüssels aufgezeigt.

Öffnen Sie den Internet Informationsdienste-Manager:

Start → Verwaltung → Internetdienstemanager

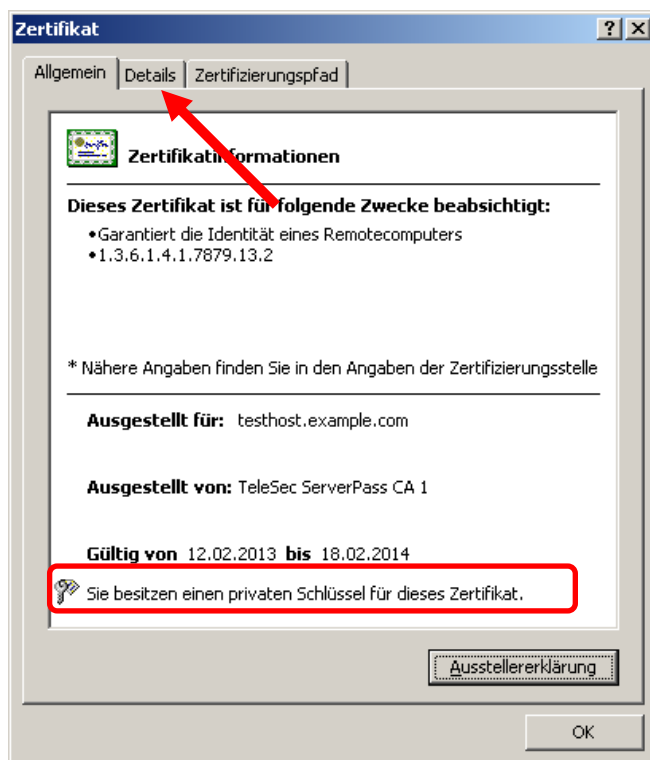
Markieren Sie die „**Standardwebseite**“ mit der rechten Maustaste und wählen dann "**Eigenschaften**". Es erscheint Abbildung 21.

Abbildung 21



Hier wählen Sie den Reiter **Verzeichnissicherheit** und schließlich **Zertifikat anzeigen**, es erscheint Abbildung 22.

Abbildung 22

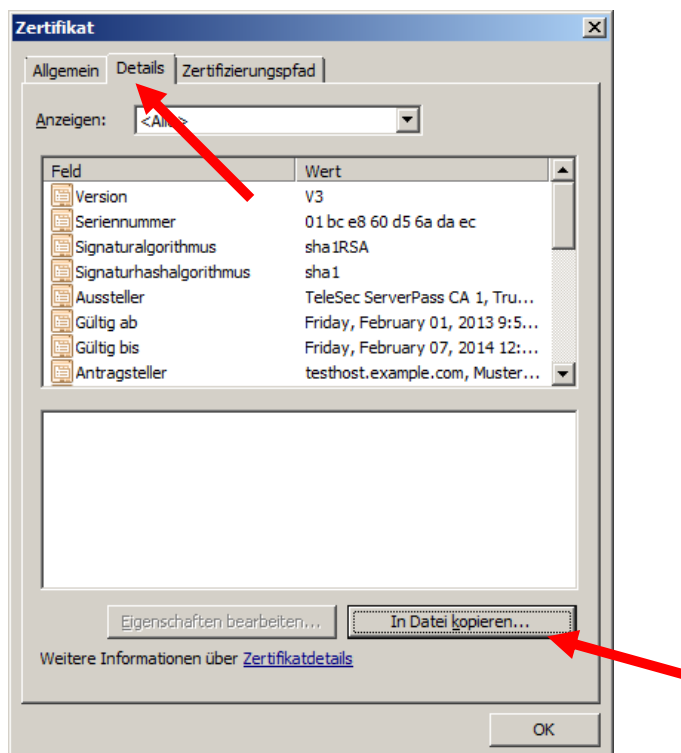


Achten Sie hier auf die korrekten Angaben für die Gültigkeit, „Ausgestellt für“ und „Ausgestellt von“.

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

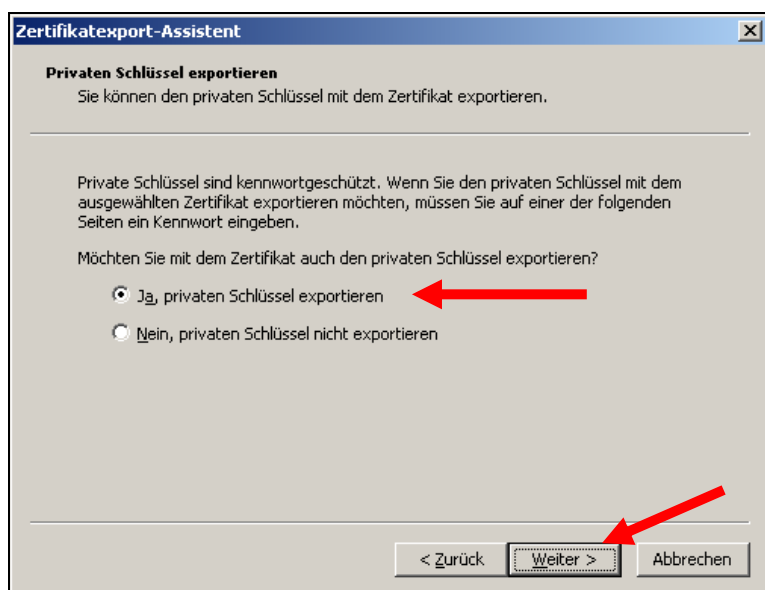
Anschließend wechseln Sie auf den Reiter **Details**, es erscheint Abbildung 23.

Abbildung 23



Wählen Sie die Option: „In Datei Kopieren“ - es öffnet sich der Zertifikatexport-Assistent, siehe Abbildung 24.

Abbildung 24:

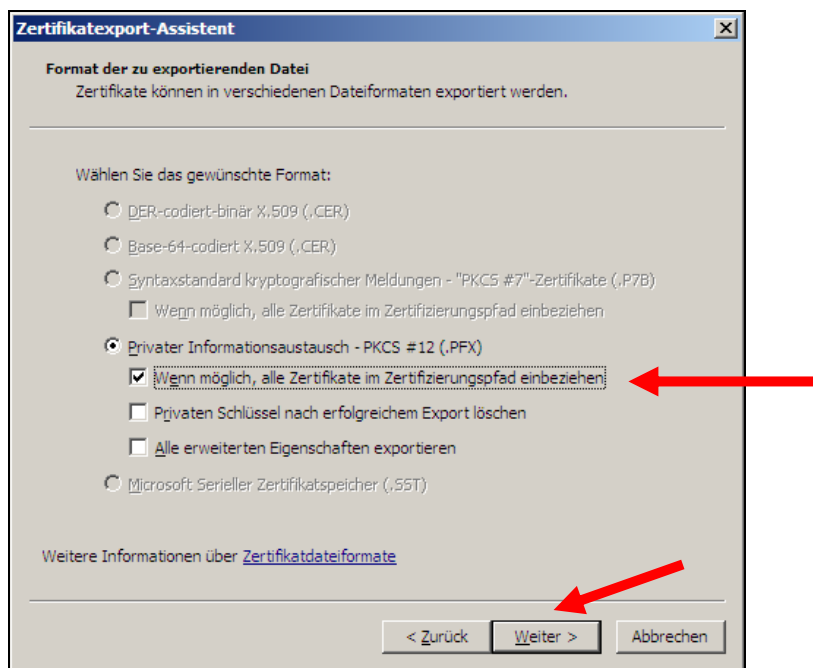


Wichtig: Im Dialogfenster **Privaten Schlüssel exportieren** wählen Sie:

„Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?“

„Ja, privaten Schlüssel exportieren“

Abbildung 25:



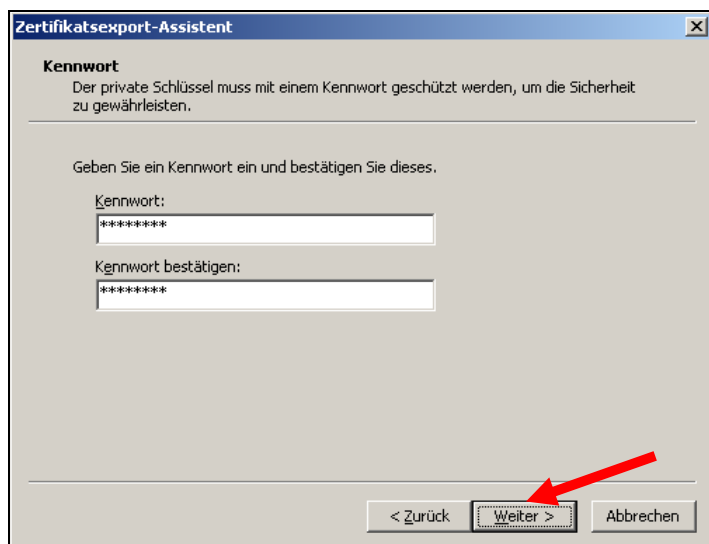
Im Dialogfenster „Format der exportierenden Datei“ wählen Sie:

„Privater Informationsaustausch – PKCS #12 (.pfx)“

Und aktivieren lediglich die Option:

„Wenn möglich alle Zertifikate im Zertifizierungspfad einbeziehen.“

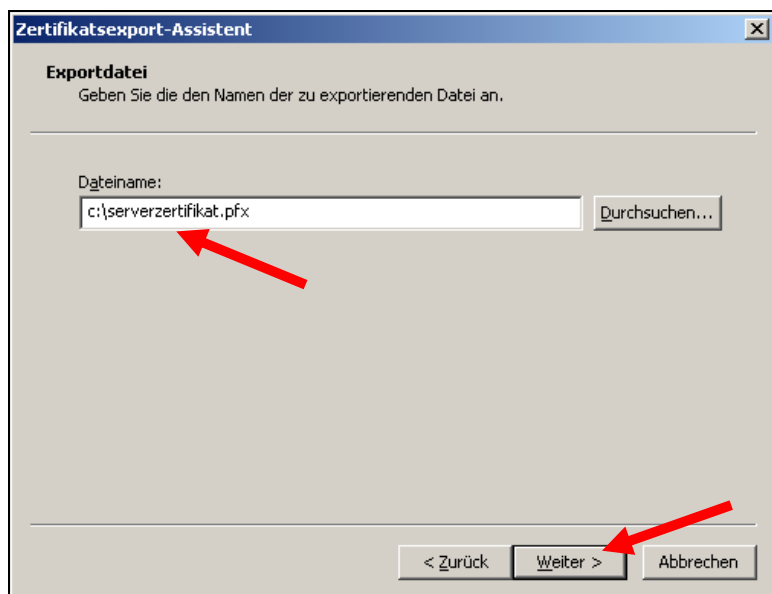
Abbildung 26:



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

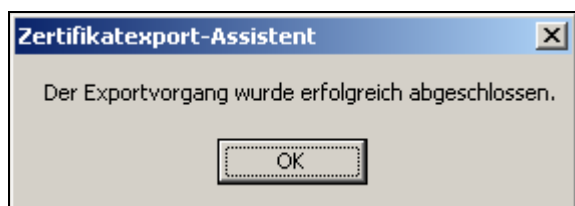
Achtung: Dieses Passwort wird bei einem ggf. erforderlichen Import benötigt!

Abbildung 27:



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

Abbildung 28



Wie in Abbildung 28 dargestellt, wird der erfolgreiche Export bestätigt.

Der Vorgang ist hiermit abgeschlossen.

3 Kontrolle

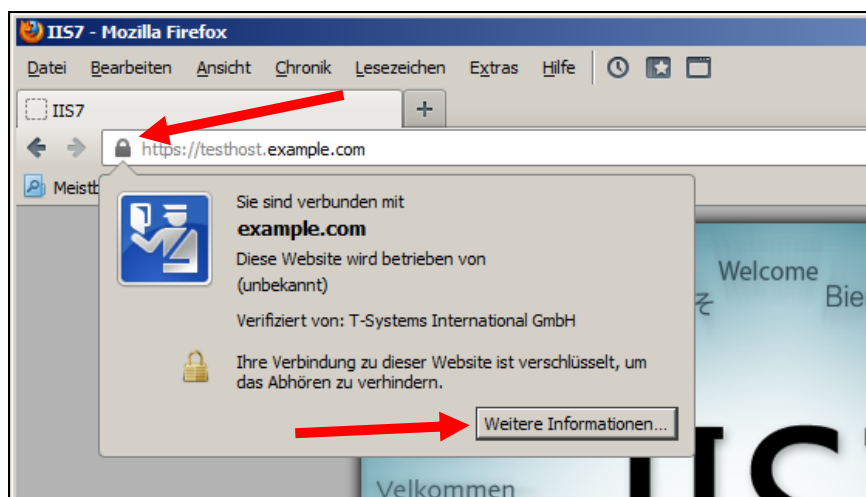
Für die Kontrolle empfiehlt sich der Aufruf der abgesicherten Webseite über einen externen Browserclient, also nicht vom Server selbst. Beim Aufruf der abgesicherten Seite, z. B. „https://testhost.example.com“ wird der SSL-Modus durch ein Schloss neben der Adressleiste symbolisiert.

Exemplarisch ist hier die Darstellung im Firefox (Abbildung 29-31) sowie im Internet Explorer (Abbildung 32-34) aufgeführt.

Andere Browser stellen den SSL-Modus ggf. anders dar.

Firefox:

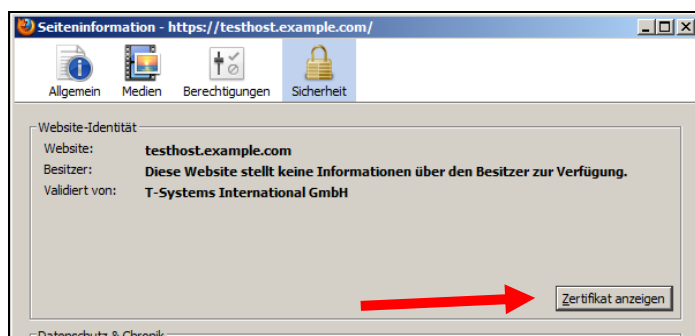
Abbildung 29 (Firefox 18):



Beim Firefox lassen sich über einen Klick auf das Schloss Details zum verwendeten Zertifikat anzeigen.

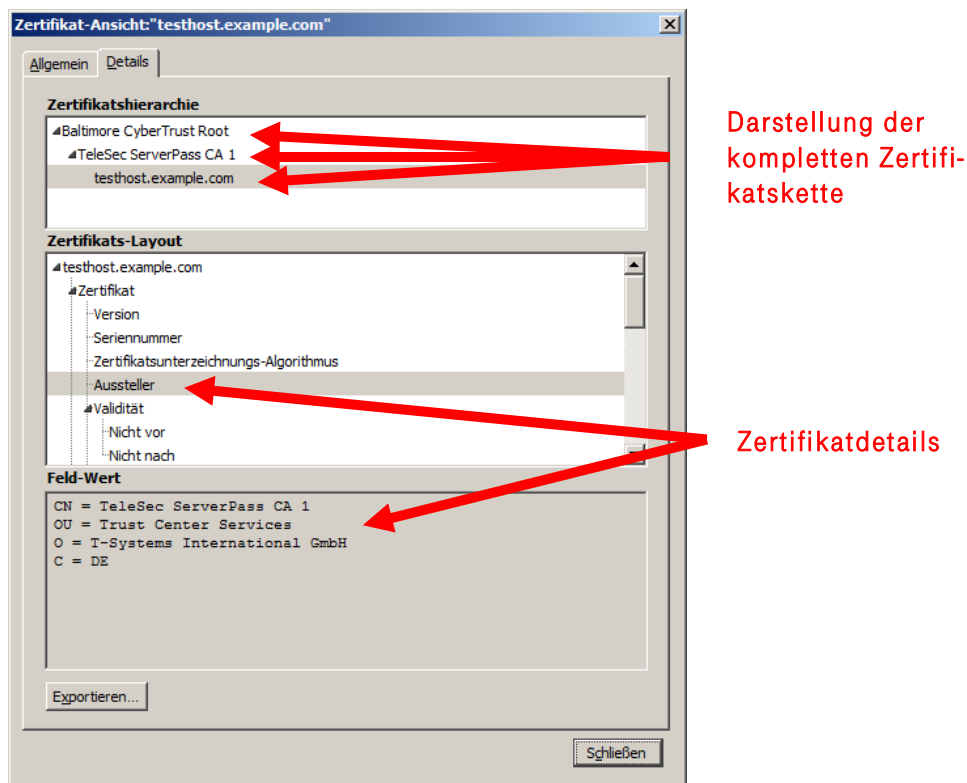
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 30 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

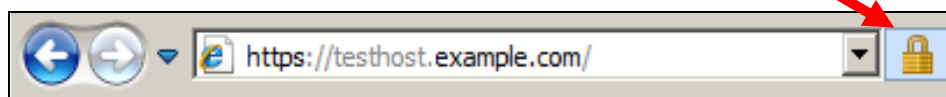
Abbildung 31 (Firefox 18):



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

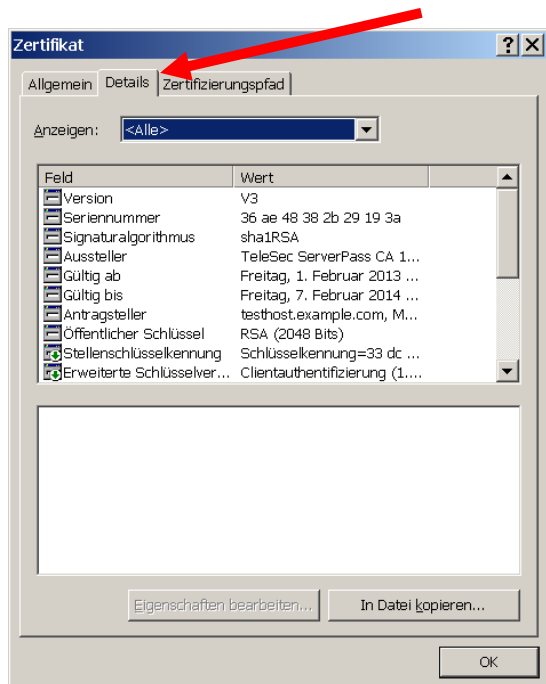
Abbildung 32 (IE 7, IE 8):



Beim Internet Explorer lassen sich die Zertifikatsdetails durch Doppelklick auf das Schloss anzeigen.

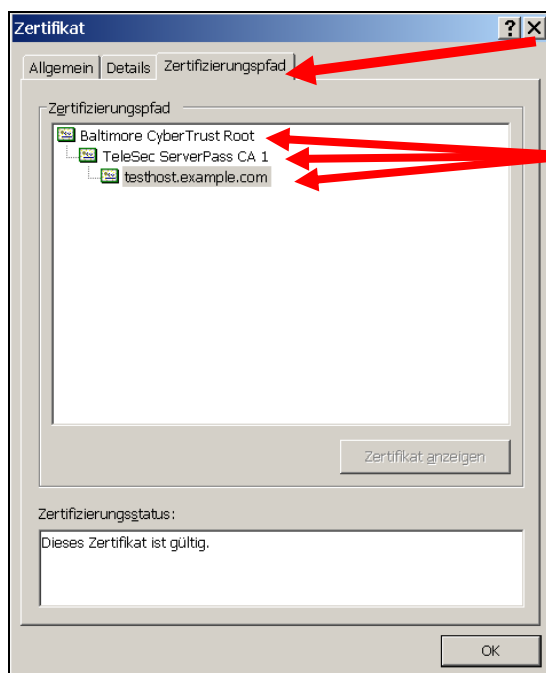
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 33.

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) V6.0“ → „Installation der CA-Zertifikate im IIS 6.0“

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