

TeleSec ServerPass

Zertifikats-Requesterzeugung für den NGINX Web-server

Version: 1.2
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-nginx.doc		Requesterzeugung NGINX Webserver

Version	Stand	Status
1.2	14.04.2014	Final

Autor	Inhaltlich geprüft von	Freigegeben von
T-Systems International GmbH GCU Midmarket Public Health & Security, PSS - Trust Center Solutions	W. Bohn	L. Eickholt

Ansprechpartner	Telefon / Fax	E-Mail
Servicedesk	Telefon: +49 (0) 1805 268 204 * * Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute	Telesec_Support@t- systems.com

Kurzinfo

Zertifikats-Requesterzeugung für den NGINX Webserver

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	05.02.2011	W. Bohn	Erster Entwurf
1.0	22.02.2011	W. Bohn	Inhalt- und Layoutanpassung
1.1	18.02.2013	W. Bohn	Inhaltliche Anpassung
1.2	10.04.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

1	Allgemeines	5
1.1	Testzertifikate.....	6
1.2	Spezielle Hinweise für NGINX Webserver	6
1.2.1	Vorbereiten des SSL-Modus	7
1.2.2	Prüfen der Systemkonfiguration.....	7
1.2.3	Dokumentenverzeichnis (DocumentRoot) für den SSL-Modus erzeugen	7
1.2.4	Konfigurationsdatei für den SSL-Modus vorbereiten	7
2	Requesterzeugung, Beauftragung, Installation, Sicherung des privaten Schlüssels	9
2.1	Requesterzeugung	9
2.1.1	(*) Stichwort „Common Name“	10
2.2	Beauftragung des Serverzertifikats	11
2.3	Herunterladen und Import der Zertifikate	13
2.3.1	Herunterladen der Zertifikate	13
2.4	Stoppen und Starten des NGINX Webservers	16
2.5	Sicherung der erzeugten Dateien	16
3	Kontrolle	17

1 Allgemeines

Dieses Dokument beschreibt die Requesterzeugung sowie die Einbindung der Zertifikate im NGINX Webserver.

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 Webserver entnehmen Sie bitte der Dokumentation des Webserver.

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, 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.

Möchten Sie für den gleichen Webserver mehrere Zertifikate beauftragen (z. B. zuerst ein Testzertifikat und anschließend ein Wirkzertifikat), so erzeugen Sie zunächst einen Request, wie in dieser Anleitung beschrieben. Soll das Zertifikat zu einem späteren Zeitpunkt durch ein anderes ersetzt werden, so muss im Server ein neuer Schlüssel und somit ein neuer Request 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 NGINX Webserver

Die Beschreibung bezieht sich auf folgende Softwarekonstellation:

NGINX Webserver 0.9.4
OpenSSL Version 1.0.1c
Plattform: Linux

Voraussetzung: Der Webserver startet bereits im unverschlüsselten Modus und alle Komponenten für den SSL-Betrieb wurden korrekt installiert.

Zur Erzeugung eines Zertifikat-Requests werden mehrere Programme angeboten. Hier dargestellt wird die Requesterzeugung mittels **OpenSSL**. Das Programm stellt eine Viel-

zahl von Optionen bereit. Weiterführende Informationen hierzu erhält man aus der Dokumentation des Programms.

Alle hier gezeigten Befehle werden innerhalb einer Eingabe-Konsole ausgeführt.

1.2.1 Vorbereiten des SSL-Modus

Damit der Webserver im SSL-Modus betrieben werden kann, sind einige Vorbereitungen erforderlich. Sollten Sie die Vorbereitungen schon durchgeführt haben, so können Sie diesen Schritt überspringen. Gezeigt wird hier lediglich eine Minimalkonfiguration, um den Webserver im SSL-Modus betreiben zu können.

1.2.2 Prüfen der Systemkonfiguration

Änderungen an Systemdateien müssen i. d. R. mit root- bzw. sudo-Rechten erfolgen! Damit der NGINX Webserver im SSL-Modus startet, müssen folgende Einträge in der nachfolgend genannten Konfigurationsdatei geprüft und ggf. gesetzt werden:

`/etc/nginx/nginx.conf`

Durch nachfolgenden Eintrag in der Datei „nginx.conf“ wird eingestellt, dass beim Starten des Webserver zusätzliche Konfigurationsdateien eingelesen werden:

```
include /etc/nginx/sites-enabled/*;
```

1.2.3 Dokumentenverzeichnis (DocumentRoot) für den SSL-Modus erzeugen

Die zu schützenden Web-Inhalte werden durch die Direktive „root“ festgelegt. Man spricht in diesem Zusammenhang auch von der „Document-Root“.

Im Beispiel liegt das Verzeichnis unter `"/usr/share/www-ssl"`, es muss ggf. erst angelegt werden, z. B. durch den Befehl `„mkdir /usr/share/www-ssl“`

1.2.4 Konfigurationsdatei für den SSL-Modus vorbereiten

Zusätzlich muss eine entsprechende Konfiguration für die Bereitstellung einer per SSL abgesicherter Webseite existieren.

Nachfolgend wird eine Grundkonfiguration aufgeführt. Diese Grundkonfiguration beschränkt sich auf das Wesentliche und dient hier lediglich zur Demonstration!

Weiterführend Informationen zur Absicherung des Webserver entnehmen Sie bitte der Dokumentation des Webserver.

Im Verzeichnis `/etc/nginx/sites-enabled` wird ein Template mit einer Grundkonfiguration für weitere Webseiten mitgeliefert, siehe Abbildung 1. Die Template-Datei trägt die Bezeichnung „default“. Es wird empfohlen, von dieser Datei zunächst eine Sicherheitskopie anzufertigen.

Nun wird die vorhandene Grundkonfiguration „default“ wie folgt angepasst:

Abbildung 1: Beispiel für eine Konfigurationsdatei

```
# HTTPS server
#
server {
    listen 443;
    server_name testhost.example.com;
    root /usr/share/nginx/www-ssl;
    index index.html index.htm;
    ssl on;
    ssl_certificate SSL/ servpass-123456-
x509chain.pem;
    ssl_certificate_key SSL/server.key;
    ssl_session_timeout 5m;
    ssl_protocols SSLv3 TLSv1;
    ssl_ciphers
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv3:+EX
P;
    ssl_prefer_server_ciphers on;
    location / {
        try_files $uri $uri/ /index.html;
    }
}
```

In der Beispieldatei „default“ werden nur Einträge bzw. Direktiven aufgelistet, die zum SSL-Betrieb unbedingt erforderlich sind. Alle anderen Einträge wurden entfernt.

Die Einträge bzw. Direktiven im Einzelnen:

- listen 443;** - Legt den SSL-Port fest, standardmäßig ist dies 443
- server_name testhost.example.com;** - Legt den Servernamen fest
- root /usr/share/nginx/www-ssl;** - Legt die „Document-Root“, den Pfad zu den Webseiten fest
- ssl on;** - legt die Betriebsart fest, SSL einschalten mit „on“
- ssl_certificate SSL/ servpass-123456-x509chain.pem;** - Legt den Pfad zur Zertifikatsdatei fest
- ssl_certificate_key SSL/server.key;** - Legt den Pfad zur Schlüsseldatei fest

Alle verfügbaren Direktiven werden in der Dokumentation des NGINX Webservers erläutert

2 Requesterzeugung, Beauftragung, Installation, Sicherung des privaten Schlüssels

2.1 Requesterzeugung

Die während der Requesterzeugung gemachten Angaben sind unveränderbar und erscheinen später im Serverzertifikat.

Vermeiden Sie die Verwendung von Feldern, die lediglich ein Leerzeichen enthalten. Soll ein Feld, z. B. „Organizational Unit“ nicht verwendet werden, so geben Sie in dieses Feld lediglich einen Punkt „.“ ein.

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>

Während der Requesterzeugung werden folgende Felder abgefragt:

Organization Name

bzw. Name der Organisation, z. B. **Musterorganisation**
Die Verwendung dieses Eintrages ist obligatorisch.

Country Name

bzw. Länderkürzel nach ISO 3166, z. B. **DE**
Die Verwendung dieses Eintrages ist obligatorisch.

Locality Name

bzw. Stadt, z. B. **Musterstadt**
Die Verwendung dieses Eintrages ist obligatorisch.

Organizational Unit Name

bzw. Name der Organisationseinheit., z. B. **Musterorgansiationseinheit**
Dieses Feld kann bis zu fünfmal vorhanden sein.
Die Verwendung dieses Eintrages ist optional.

State or Province

bzw. Bundesland, z. B. **Bundesland**
Die Verwendung dieses Eintrages ist obligatorisch.

Postal Code

bzw. Postleitzahl, z. B. **12345**
Die Verwendung dieses Eintrages ist optional.

Street Name

bzw. Straßenname, z. B. **Musterstrasse**

Die Verwendung dieses Eintrages ist optional.

Common Name (*)

bzw. Gemeinsamer Name, z. B. **testhost.example.com**

Die Verwendung dieses Eintrages ist obligatorisch, siehe Punkt 2.1.1

Email Address

bzw. Emailadresse, z. B. **meine.email@provider**

Challenge Password

bzw. Zusätzliches Passwort: nicht erforderlich, nur Return drücken

Optional Company Name

bzw. Optionaler Firmenname: nicht erforderlich, nur Return drücken

Je nach Konfiguration ist die Abfrage weiterer Angaben möglich.

2.1.1 (*) Stichwort „Common Name“

Für den "Common Name" ist die Adresse des Servers einzutragen, die verschlüsselt werden soll, z.B. **www.telesec.de**

(In der Regel ist dies der „FQDN“, der **Fully Qualified Domain Name** 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.

Das folgende Kommando erzeugt einen Server-Schlüssel ohne Passwortschutz und einen Server-Zertifikat-Request:

openssl req -newkey rsa:2048 -keyout server.key -nodes -new -out requestdatei.pem

Soll ein Server-Schlüssel mit Passwortschutz erzeugt werden (der Webserver lässt sich nur nach Eingabe des Passwortes starten), verwenden Sie dieses Kommando:

openssl req -newkey rsa:2048 -keyout server.key -new -out requestdatei.pem

Die Zahl im Kommando legt die verwendete Bitlänge (Schlüssellänge) des Server-Schlüssels und damit des Requests fest. Mögliche Werte sind: 2048 oder 4096.

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

Durch das Kommando sind folgende Dateien entstanden:

Die Server-Zertifikat-Request Datei: **requestdatei.pem**

Die Server-Schlüssel-Datei: **server.key**

Die Datei „requestdatei.pem“ beinhaltet den Request in der angegebenen Form:

Abbildung 2 (requestdatei.pem)

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIBxzCCAttrtTACAQAwwYYxCzAJBgNVBAYTAkRFRMQwwCgYDVQQIEANBgNV  
....  
DGysW9I7Wv9SOeW5HrhL4SIlzVVVzFUW5NvRpQCaE+qIkpo+w9l5K0/HFn5mWSkT  
cPMXx5uYkJNO8l9REmvcJMhvJIzw4vP+kyjM  
-----END CERTIFICATE 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 2 inklusive der „-----BEGIN....“ und „-----END...“ Zeilen per cut & paste.

Nach dem Einfügen werden die Request-Inhalte zur Kontrolle angezeigt, siehe Abbildung 3.

Abbildung 3



Füllen Sie alle weiteren Felder entsprechen Ihren 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. 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 der Zertifikate

2.3.1 Herunterladen der Zertifikate

Anmelden im Webportal „myServerPass“:

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

Wählen Sie den Menüpunkt „Meine Zertifikate“

Hier werden nun alle Ihre Zertifikate aufgelistet, siehe Abbildung 4.

Abbildung 4

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

Wählen Sie das herunterzuladende Zertifikat durch Klick auf die Referenznummer aus, siehe Abbildung 4.

Abbildung 5

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.	
<input type="button" value="Download (nur Zertifikat)"/> <input type="button" value="Download (inkl. Zertifikatskette)"/> <input type="button" value="Sperren"/> <input type="button" value="Verlängern"/> <input type="button" value="Abbrechen"/>	

Wie in Abbildung 5 gezeigt, werden die Zertifikatsdaten zur Kontrolle angezeigt.

Angeboten werden zwei Download-Formate:

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

Abbildung 6 (servpass-123456-x509chain.pem)

```
# Ihr ServerPass Zertifikat:
# -----
# Subject:
C=DE,O=Musterorganisation,OU=Musterorganisationseinheit,ST=Bundesland,L=Musterstadt,
CN=testhost.example.com
# Issuer: C=DE,O=T-Systems International GmbH,OU=Trust Center Services,CN=TeleSec
ServerPass CA 1
# Ser.No.: 0x01bce860d56adaec
-----BEGIN CERTIFICATE-----
MIIFxiCCBK6gAwIBAgICQBMwDQYJKoZIhvcNAQEFBQAwYlxCzAJBgNVBAYTAkRF
...
OGAb1gNE4cu5uYPKtTLbFVyaZ6EhHUoM00Vwl63IU9TUhC1rEUZUb5HI
-----END CERTIFICATE-----
-----# CA Zertifikat:
# CA Zertifikat:
#-----
# Subject: C=DE,O=T-Systems International GmbH,OU=Trust Center Services,CN=TeleSec
ServerPass CA 1
# Issuer: C=IE,O=Baltimore,OU=CyberTrust,CN=Baltimore CyberTrust Root
# Ser.No.: 0x072742c2
-----BEGIN CERTIFICATE-----
IkJlhGUKjhljLKLKKJLKhguGugtuigjkZIU
...
9OuONM/anP8/AdEIZ6ziGwdUpRzLIO8eA==
-----END CERTIFICATE-----
#
# Root Zertifikat:
# -----
# Subject: C=IE,O=Baltimore,OU=CyberTrust,CN=Baltimore CyberTrust Root
# Issuer: C=IE,O=Baltimore,OU=CyberTrust,CN=Baltimore CyberTrust Root
# Ser.No.: 0x020000b9
-----BEGIN CERTIFICATE-----
MIIDdTCCA12gAwIBAgILAgAAzELMAkG
...
Zg6C3ZjL2sJETy6ge/L3ayx2EYRGinij4w==
-----END CERTIFICATE-----
```

Schlüssel- und Zertifikatsdatei können nun gemäß der SSL-Direktiven abgespeichert bzw. die Direktiven wir folgt gesetzt werden:

ssl_certificate /etc/nginx/SSL/servpass-123456-x509chain.pem;

ssl_certificate_key SSL/server.key;

Anschließend muss der Webserver neu gestartet werden, siehe 2.4

2.4 Stoppen und Starten des NGINX Webservers

Der NGINX Webserver muss zunächst gestoppt und anschließend wieder gestartet werden:

Webserver stoppen: **nginx -s stop**

Webserver starten: **nginx**

Wurde der Schlüssel mit Passwortschutz erzeugt, wird für den Start und auch das Beenden das Passwort des Server-Schlüssels abgefragt.

2.5 Sicherung der erzeugten Dateien

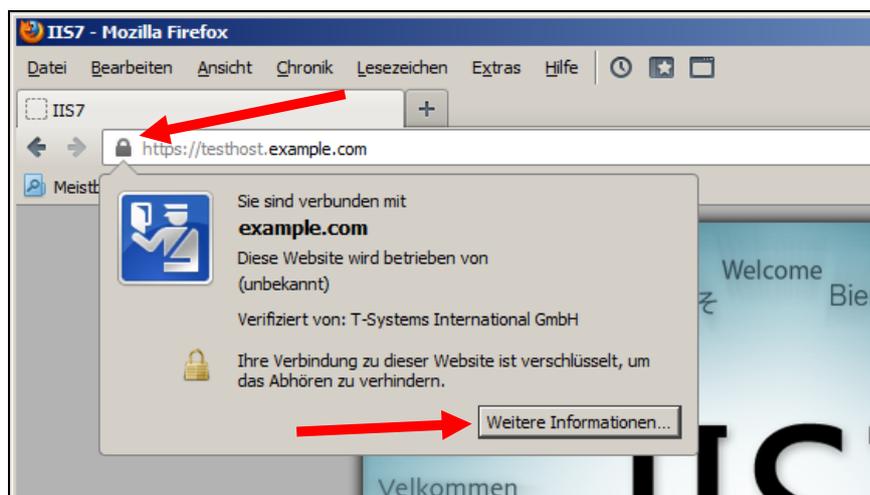
Es wird empfohlen, die erzeugten Schlüssel- und Zertifikats-Dateien zu sichern, z. B. auf einem externen Medium!

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 Adresleiste symbolisiert. Andere Browser stellen den SSL-Modus ggf. anders dar. Exemplarisch ist hier die Darstellung im Firefox (Abbildung 7-9) sowie im Internet Explorer (Abbildung 10-12) aufgeführt.

Firefox:

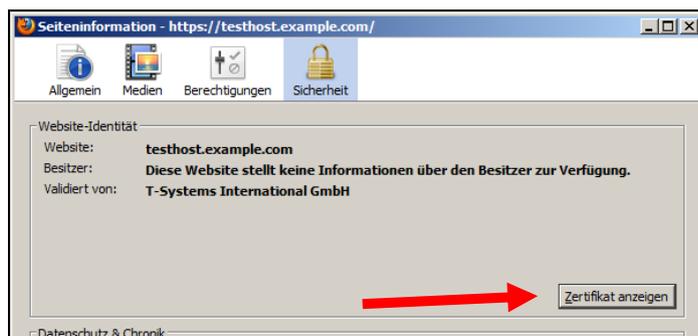
Abbildung 7 (Firefox 18):



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

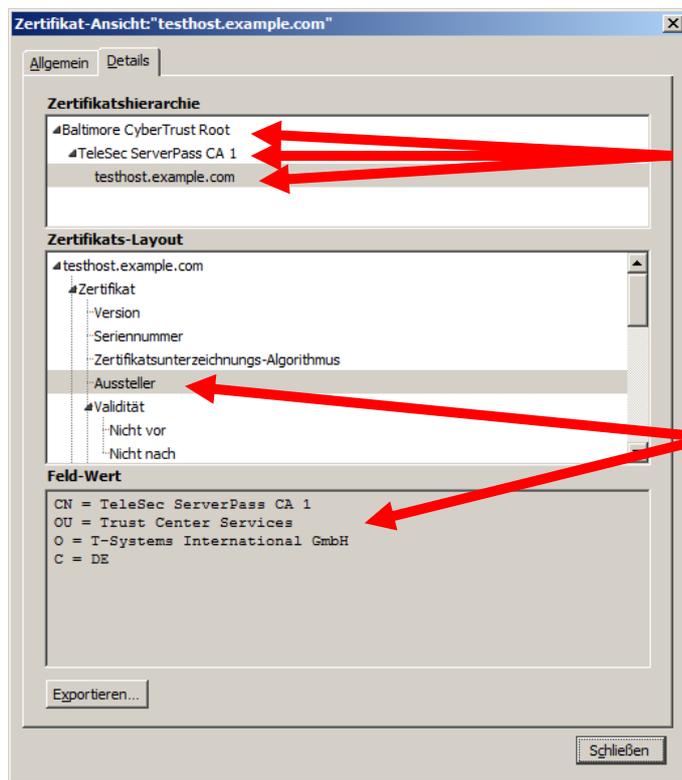
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 8 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

Abbildung 9 (Firefox 18):



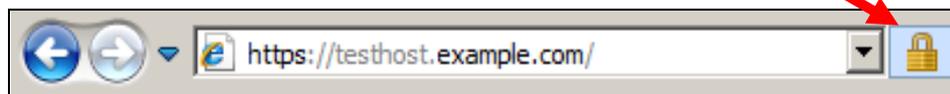
Darstellung der kompletten Zertifikatskette

Zertifikatdetails

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

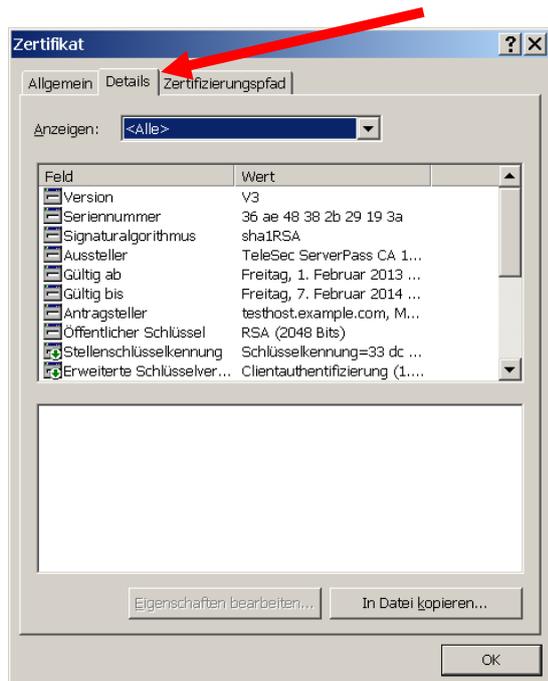
Abbildung 10 (IE 7, IE 8):



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

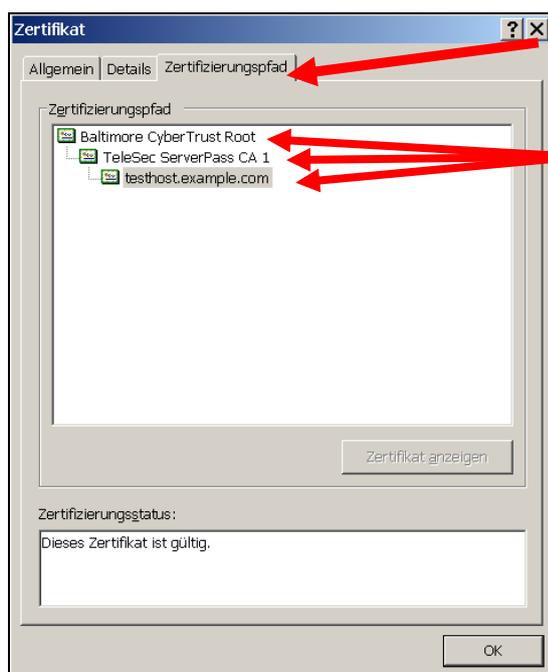
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 11.

Abbildung 11 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 12.

Abbildung 12 (Die Zertifikatskette)



Darstellung der kompletten Zertifikatskette

So wie in Abbildung 12 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.