TeleSec ServerPass

Zertifikats-Requesterzeugung für den Apache 2 Webserver

Version: 1.5
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_req_inst-apache2.doc		Requesterzeugung Apache 2 Webserver

Version	Stand	Status
1.5	14.04.2014	Final

Autor	Inhaltlich geprüft von	Freigegeben von
T-Systems International GmbH ICT Operation, PSS – Professional Services & Solutions Trust Center Services	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 Apache 2 Webserver

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	15.09.2009	W. Bohn	Erster Entwurf
1.0	30.04.2010	W. Bohn	Inhalt- und Layoutanpassung
1.1	07.01.2011	W. Bohn	Inhaltliche Anpassung
1.2	20.01.2011	W. Bohn	Inhaltliche Anpassung
1.3	27.01.2011	W. Bohn	Inhaltliche Anpassung
1.4.	11.02.2013	W. Bohn	Inhaltliche Anpassung
1.5	10.04.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

1 Allgemeines 5

1.1 Testzertifikate ... 6

1.2 Spezielle Hinweise für Apache 2 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 10

2.1 Requesterzeugung ... 10

2.1.1 (*) Stichwort „Common Name“ ... 11

2.2 Beauftragung des Serverzertifikats ... 12

2.3 Herunterladen und Import der Zertifikate ... 14

2.3.1 Herunterladen der Zertifikate ... 14

2.3.1a Die aktuellen Root- und CA-Zertifikate werden auf Ihrem Apache Webserver schon eingesetzt. ... 15

2.3.1b Die aktuellen Root- und CA- Zertifikate werden noch nicht auf Ihrem Apache Webserver schon eingesetzt ... 15

2.4 Starten des Apache Webservers im SSL-Modus ... 18

2.5 Sicherung der erzeugten Dateien ... 18

3 Kontrolle 19

1 Allgemeines

Dieses Dokument beschreibt die Requesterzeugung sowie die Einbindung der Zertifikate im Apache 2 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 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, 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 Apache 2 Webserver

Die Beschreibung bezieht sich auf folgende Softwarekonstellation:

Apache Webserver 2.2.8
OpenSSL Version 1.0.1c
Plattform: Linux bzw. Unix

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.

1.2.2 Prüfen der Systemkonfiguration

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

/etc/sysconfig/apache2

Das Laden des SSL-Moduls ist zwingend erforderlich:

Hierzu muss der Parameter **APACHE_MODULES** den Eintrag **„ssl“** enthalten, z. B:

APACHE_MODULES=“…actions alias auth_basic ssl suexec userdir…“

Optional kann der Webservers standardmäßig im SSL-Modus gestartet werden:

Hierzu wird der Parameter: **APACHE_SERVER_FLAGS** wird wie folgt gesetzt**:**

APACHE_SERVER_FLAGS="SSL“

1.2.3 Dokumentenverzeichnis (DocumentRoot) für den SSL-Modus erzeugen

Die zu schützenden Web-Inhalte werden durch die Direktive „DocumentRoot“ festgelegt. Im Beispiel liegt das Verzeichnis unter "/srv/www/htdocs-ssl”, es muss ggf. erst angelegt werden, z. B. durch den Befehl „mkdir /srv/www/htdocs-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 Webservers entnehmen Sie bitte der Dokumentation des Webservers.

Im Verzeichnis /etc/apache2/vhosts wird ein Template einer Grundkonfiguration für den SSL-Modus mitgeliefert, siehe Abbildung 1.

Man kann die vorhandene Grundkonfiguration wie folgt kopieren:
cp vhost-ssl.template vhosts-ssl.conf
Wichtig ist hierbei die Endung „.conf“, nur so wird die Datei als Konfigurationsdatei erkannt und beim Starten des Webservers eingelesen.

Abbildung 1: Beispiel für eine Konfiguration “vhosts-ssl.conf”

```
<IfDefine SSL>
<IfDefine !NOSSL>

<VirtualHost _default_:443>

    DocumentRoot "/srv/www/htdocs-ssl"
    ServerName localhost:443
    ServerAdmin root@domain
    ErrorLog /var/log/apache2/error_log
    TransferLog /var/log/apache2/access_log

<Directory />

  AllowOverride none
  Order allow,deny
  allow from all
</Directory>

    SSLEngine on

    SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

    SSLCertificateFile /etc/apache2/ssl.crt/server.crt
    SSLCertificateKeyFile /etc/apache2/ssl.key/server.key
    SSLCertificateChainFile /etc/apache2/ssl.crt./ca.crt

    <Files ~ "\.(cgi|shtml|phtml|php3?)$">
       SSLOptions +StdEnvVars
    </Files>
    <Directory "/srv/www/cgi-bin">
       SSLOptions +StdEnvVars
    </Directory>

    SetEnvIf User-Agent ".*MSIE.*" \
          nokeepalive ssl-unclean-shutdown \
          downgrade-1.0 force-response-1.0

    CustomLog /var/log/apache2/ssl_request_log   ssl_combined

</VirtualHost>

</IfDefine>
</IfDefine>
```

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 (**C**ertificate **P**ractice **S**tatement) aufgeführten Hinweise. Insbesondere den erlaubten Zeichensatz.

Siehe hierzu: http://www.telesec.de/serverpass/cps.html

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 Adress
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. 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“ 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).

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

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

Soll ein Server-Key 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-Keys 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-----
MIIBxzCCAtrrtTACAQAwgYYxCzAJBgNVBAYTAkRFMQwwCgYDVQQIEANBgNV
....
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

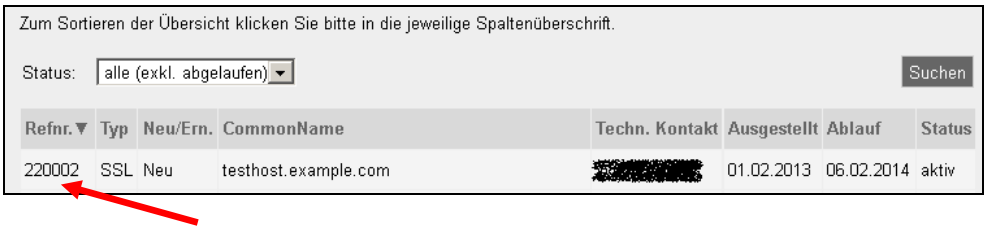
2.3.1 Herunterladen der Zertifikate

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

Wählen Sie den Menüpunkt „Meine Zertifikate“

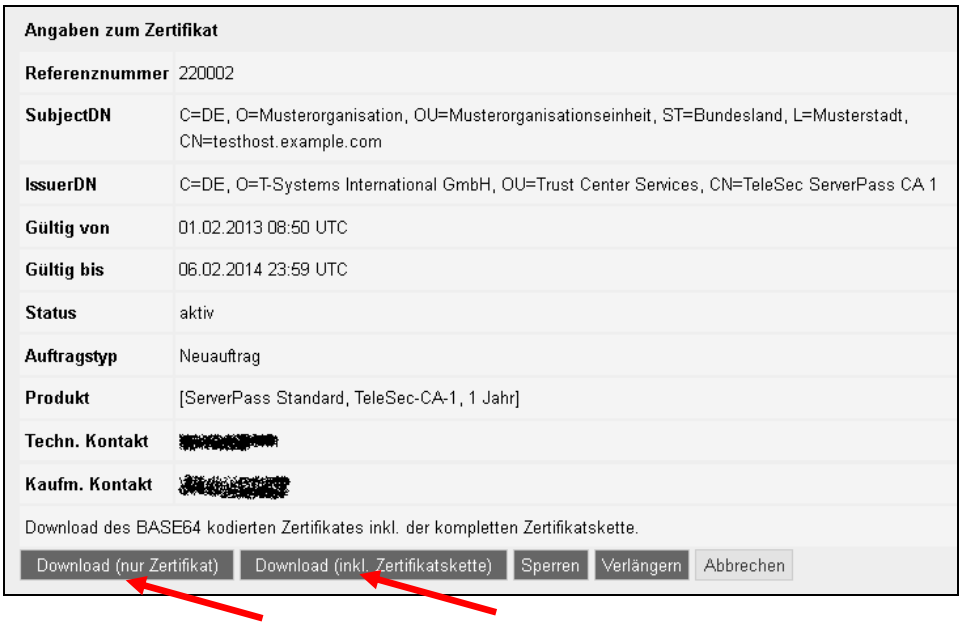
Hier werden nun alle Ihre Zertifikate aufgelistet.

Abbildung 4:



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

Abbildung 5



Wie in Abbildung 5 gezeigt, werden die Zertifikatsdaten zur Kontrolle angezeigt. Angeboten werden zwei Download-Formate:

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

2.3.1a Die aktuellen Root- und CA-Zertifikate werden auf Ihrem Apache Webserver schon eingesetzt.

Sofern im Apache 2 Webserver bereits die aktuellen Root- und CA-Zertifikate zum Einsatz kommen laden Sie lediglich das Zertifikat herunter „Download (nur Zertifikat)“.
Aktivieren Sie die Option „Als Datei speichern und legen einen Dateipfad fest, z. B. /etc/apache2/
Sie erhalten die Datei „servpass-123456-x509.pem“ und sie liegt nun in diesem Verzeichnis: /etc/apache2/

Passen Sie die Direktive **SSLCertificateFile** bzw. die dort verwendete Datei an.
Falls schon eine Zertifikatsdatei existiert, so sollten Sie zunächst eine Sicherheitskopie dieser Datei anfertigen, z. B. durch diesen Befehl: „cp server.crt server.crt.old“.
Anschließend wir die herunter geladene Datei an die Stelle des zu erneuernden Zertifikats kopiert, die ursprüngliche Datei wird hierbei überschrieben:
„cp /etc/apache2/servpass-123456-x509.pem /etc/apache2/ssl.crt/server.crt

Nun muss der Webserver neu gestartet werden, siehe 2.4

2.3.1b Die aktuellen Root- und CA- Zertifikate werden noch nicht auf Ihrem Apache Webserver schon eingesetzt

Werden die aktuellen Root- und CA-Zertifikate noch nicht eingesetzt, so wählen Sie das Format: „Download inkl. Zertifikatskette“.
Aktivieren Sie die Option „Als Datei speichern und legen einen Dateipfad fest, z. B. /etc/apache2/
Sie erhalten die Datei „servpass-123456-x509chain.pem“ und sie liegt nun in diesem Verzeichnis: /etc/apache2/

So wie in Abbildung 6 dargestellt, enthält die herunter geladene Datei mehrere Zertifikate. Im Einzelnen sind dies:

1. Das eigentliche „Serverzertifikat“, auch User-Zertifikat genannt.
2. Das Zertifikat „TeleSec ServerPass CA 1“, auch CA-Zertifikat genannt.
3. Das Zertifikat „Baltimore CyberTrust Root“ Zertifikat, auch Root-Zertifikat genannt.

Abbildung 6 (servpass-123456-x509chain.pem)

```
# Ihr ServerPass Zertifikat:
# -------------------------
#   Subject: #   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-----
MIIFxjCCBK6gAwIBAgICQBMwDQYJKoZIhvcNAQEFBQAwgYIxCzAJBgNVBAYTAkRF
...
OGAb1gNE4cu5uYPKtTLbFVyaZ6EhHUoM00Vwl63lU9TUhClrEUZUb5HJ
-----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-----
lkjlhGUkjhkljLKLKKJJLKhguGugtuigjkZIU.
...
9OuONM/anP8/AdEIZ6ziGwdUpRzLlO8eA==
-----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-----
MIIDdTCCAl2gAwIBAgILAgAAzELMAkG
...
Zg6C3ZjL2sJETy6ge/L3ayx2EYRGinij4w==
-----END CERTIFICATE-----
```

Öffnen Sie die herunter geladene Datei mit einem einfachen Texteditor z. B. „vi“ oder Wordpad, ggf. muss bei Öffnen der Dateityp „Alle Dokument *.*“ eingestellt werden. Markieren Sie das Server bzw. User-Zertifikat incl. der ---BEGIN... und ---END... Zeilen (hier blau unterlegt) und speichern es als Textdokument in einer eigene Datei ab, z. B. „server.crt.neu“, siehe Abbildung 7.

Abbildung 7: (server.crt.neu)

```
-----BEGIN CERTIFICATE-----
MIIE1DCCA7ygAwIBAgILBAAAAAABC
...
qBj2G5mCE4T12MweD3l+S9OuONM/anP8/
 -----END CERTIFICATE-----
```

Das Serverzertifikat

Nach dem gleichen Schema werden nun CA- und Root-Zertifikat behandelt:

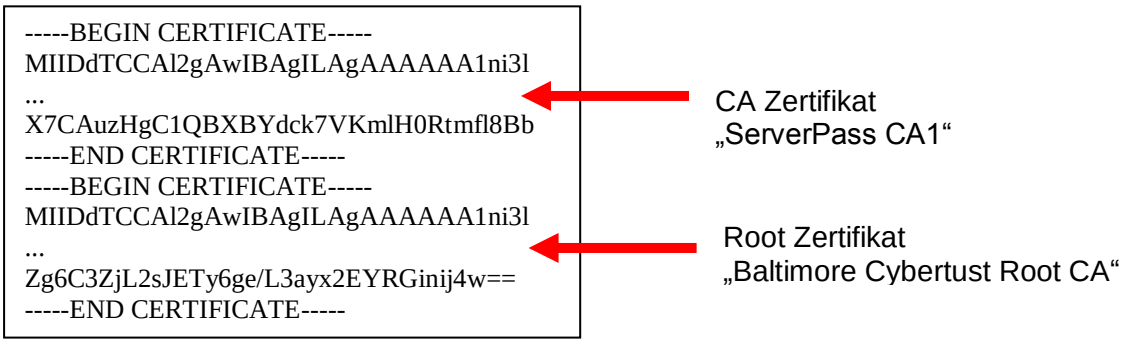
CA-Zertifikat: Markieren Sie das CA-Zertifikat „TeleSec ServerPass CA 1“ incl. der ---BEGIN... und ---END... Zeilen (hier magenta markiert) und speichern es als Textdokument in eine eigene Datei ab, z. B. „ServerPass-CA1.crt“. Sollten in der herunter geladenen Datei mehrere CA-Zertifikate aufgelistet werden, so verfahren Sie mit diesen CA-Zertifikaten analog.

Root-Zertifikat: Markieren Sie das Root-Zertifikat „Baltimore Cybertrust Root CA“ incl. der ---BEGIN... und ---END... Zeilen (hier grün markiert) und speichern es als Textdokument in eine eigene Datei ab, z. B. „BaltimoreCyberustRoot.crt“

CA- und Root-Zertifikat können auch in einer einzigen Datei geführt werden. Hierzu kopieren Sie das Root-Zertifikat (hier grün unterlegt) direkt unter die schon vorhandenen Zertifikate. Wird bereits solch eine Datei verwendet, so können Sie das Root- und CA-Zertifikat hinten anfügen.

Die Datei „ca.crt“ hat nun den in Abbildung 8 gezeigten Aufbau.

Abbildung 8 (ca.crt)



Falls schon eine Zertifikatsdatei existiert, so sollten Sie zunächst eine Sicherheitskopie dieser Datei anfertigen, z. B. durch diesen Befehl:
„cp server.crt server.crt.old“.
Anschließend wir die soeben erzeugte Datei an die Stelle des zu erneuernden Zertifikats kopiert, die ursprüngliche Datei wird hierbei überschrieben:
„cp server.crt.neu /etc/apache2/ssl.crt/server.crt“

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

SSLCertificateFile /etc/apache2/ssl.crt/server.crt

SSLCertificateKeyFile /etc/apache2/ssl.key/server.key

SSLCertificateChainFile /etc/apache2/ssl.crt./ca.crt

Bedeutung der Direktiven:

SSLCertificateFile	zeigt auf das Serverzertifikat aus der heruntergeladenen Datei, z. B. **server.crt**
SSLCertificateKeyFile	zeigt auf den Serverkey: z. B. **server.key**
SSLCertificateChainFile(*)	zeigt auf die Datei **ca.crt**

(*) Die Verwendung der Direktive SSLCertificateChainFile wird unbedingt empfohlen!

Der Webserver präsentiert dann neben dem User-Zertifikat auch Zertifikate der ausstellenden Instanz(en), siehe Abbildung 11 bzw. 14. Jedoch wird diese Direktive von einigen älteren Server-Versionen nicht unterstützt.

Anschließend muss der Webserver neu gestartet werden, siehe 2.4

2.4 Starten des Apache Webservers im SSL-Modus

Der Apache Webserver muss zunächst gestoppt und anschließend wieder gestartet werden:
/etc/init.d/apache2 **stop**
/etc/init.d/apache2 **start**

Andere Startbefehle sind ebenfalls möglich, z. B.
/etc/init.d/apache2 **stop**
/etc/init.d/apache2 **startssl**

Wurde der Schlüssel mit Passwortschutz erzeugt, wird für den Start das Passwort des Server-Keys abgefragt.

2.5 Sicherung der erzeugten Dateien

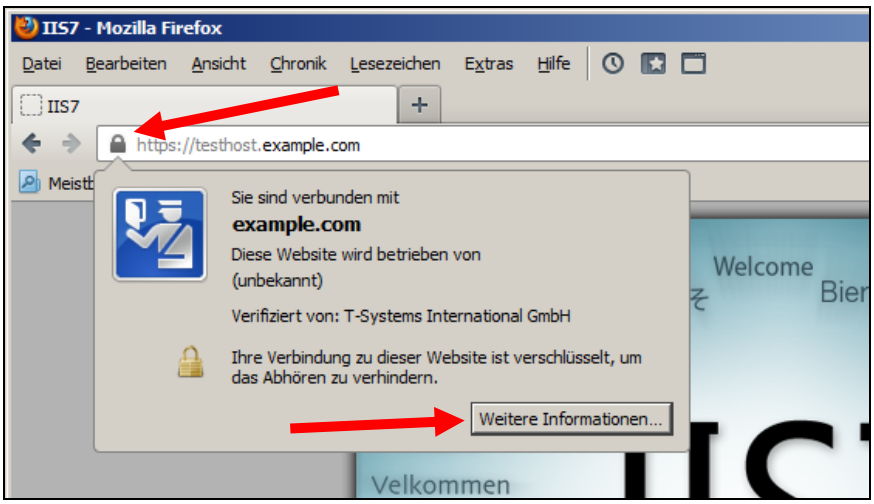
Es wird empfohlen, die erzeugten Schlüssel- und Zertifikats-Dateien zu sichern, z. B. auf einem externen Medium!

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 Adressleiste symbolisiert. Andere Browser stellen den SSL-Modus ggf. anders dar. Exemplarisch ist hier die Darstellung im Firefox (Abbildung 9-11) sowie im Internet Explorer (Abbildung 12-14) aufgeführt.

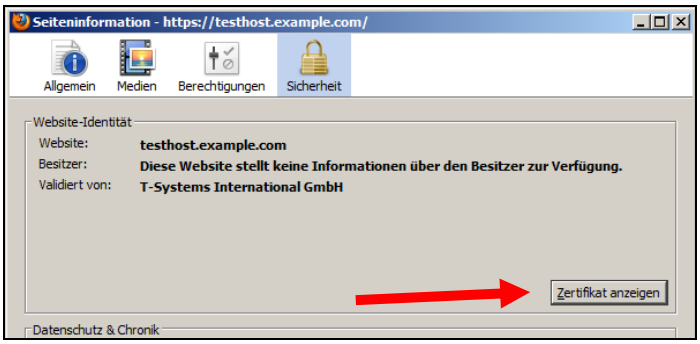
Firefox:

Abbildung 9 (Firefox 18):



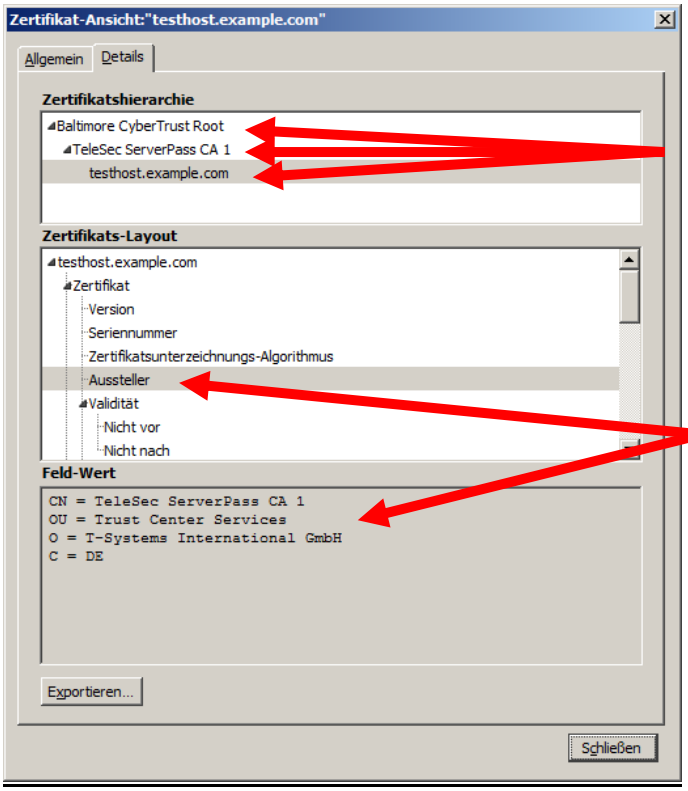
Beim Firefox lassen sich über einen Klick auf das Schloss Details zum verwendeten Zertifikat anzeigen.
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 10 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

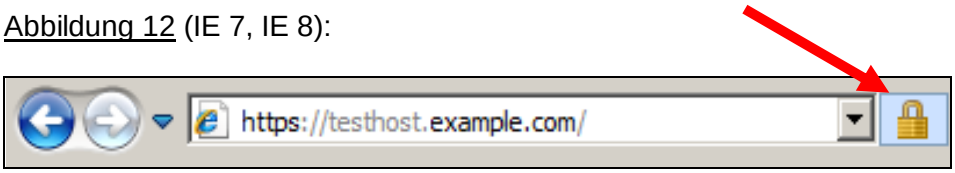
Abbildung 11 (Firefox 18):



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“

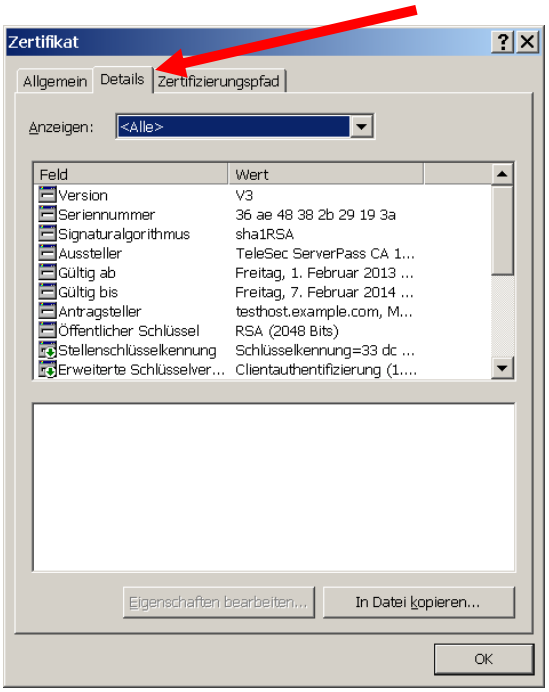
Internet Explorer

Abbildung 12 (IE 7, IE 8):



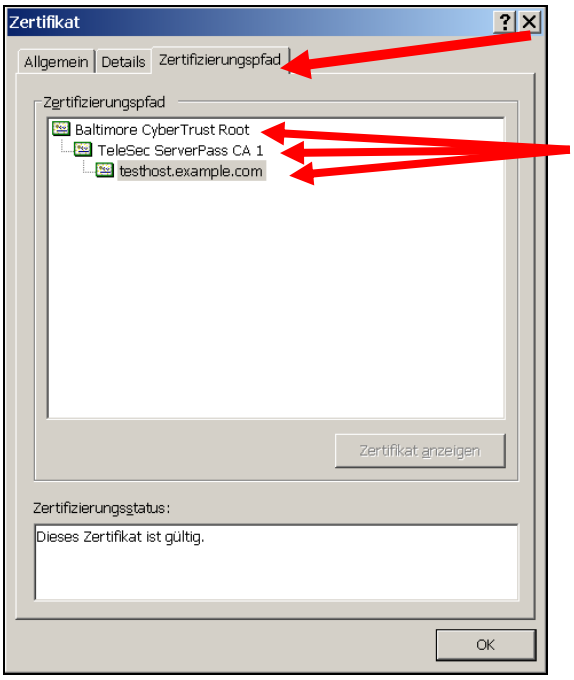
Beim Internet Explorer lassen sich die Zertifikatsdetails durch Doppelklick auf das Schloss anzeigen.
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 13.

Abbildung 13 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 14.

Abbildung 14 (Die Zertifikatskette)



Darstellung der kompletten Zertifikatskette

So wie in Abbildung 14 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.