

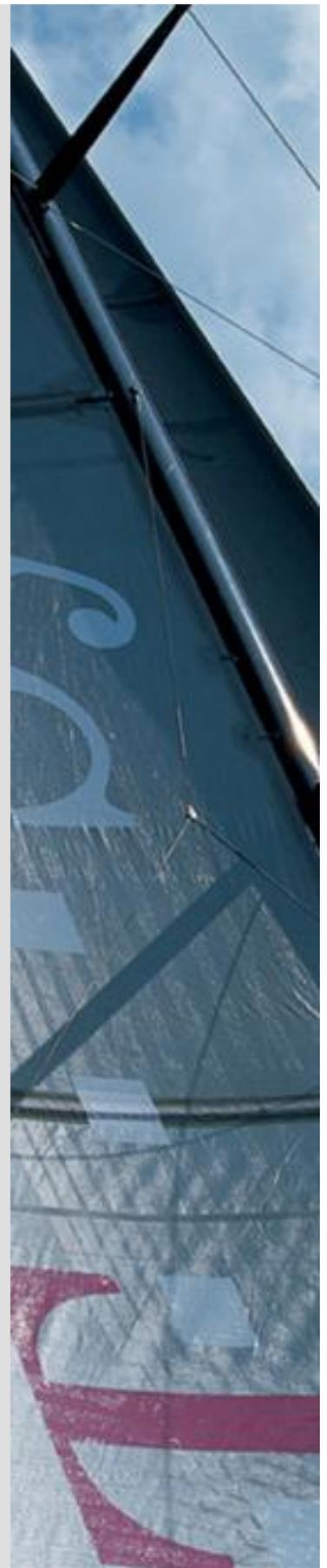
TeleSec ServerPass

Zertifikatserneuerung 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_erneu_inst-apache2.doc		Zertifikatserneuerung 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

Zertifikatserneuerung 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
2	Erneuerung, Beauftragung, Installation, Sicherung des privaten Schlüssels	7
2.1	Bedingungen für eine Zertifikatserneuerung	7
2.2	Besonderer Hinweis für eine Zertifikats-Erneuerung unter Apache 2 Webserver.....	8
2.3	Erneuerung durchführen	8
2.3.0	Die Verwendung des Public Keys bei der Erneuerung.....	11
2.3.1	Erneuerung unter Wiederverwendung des Public Keys.....	11
2.3.2	Erneuerung unter Verwendung eines neuen Public Keys.....	11
2.4	Import des erneuerten Zertifikats	13
2.4.1	Herunterladen des erneuerten Zertifikats.....	13
2.4.1a	Die aktuellen Root- und CA-Zertifikate werden auf Ihrem Apache Webserver schon eingesetzt.....	14
2.4.1b	Die aktuellen Root- und CA- Zertifikate werden noch nicht auf Ihrem Apache Webserver schon eingesetzt.....	15
2.5	Starten des Apache Webservers im SSL-Modus.....	18
2.6	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 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.

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 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 läuft bereits im SSL-Modus unter Verwendung eines TeleSec ServerPass Serverzertifikats.

Zur Erzeugung eines Zertifikat-Requests werden mehrere Programme angeboten. Hier dargestellt wird die Requesterzeugung mittels **OpenSSL**. Das Programm stellt eine Vielzahl von Optionen bereit. Weiterführende Informationen hierzu erhält man aus der Dokumentation des Programms.

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

2 Erneuerung, Beauftragung, Installation, Sicherung des privaten Schlüssels

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 einer 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 Server-Schlüssels sowie eines neuen Zertifikat-Requests erforderlich. Folgen Sie hierzu bitte der Anleitung:

„Apache 2 Webserver“ → „Zertifikat-Requesterzeugung, Installation der Zertifikate“

2.2 Besonderer Hinweis für eine Zertifikats-Erneuerung unter Apache 2 Webserver

In der Regel ist die Erzeugung eines weiteren Requests nicht erforderlich.
 Sollte dennoch ein neuer Request erzeugt werden, so erzeugen Sie bitte eine neue Zertifikatsanforderung, gemäß Anleitung „Apache 2 Webserver -> Zertifikat-Requesterzeugung, Installation der Zertifikate“.
 Beachten Sie, dass während der Requesterzeugung die gleichen Angaben (Organisation, Organisationseinheit, Common Name, Stadt, Bundesland, Staat, evtl. auch Strasse und Postleitzahl) gemacht werden müssen, wie bei der Beauftragung des zu erneuernden TeleSec ServerPass Zertifikats. Ansonsten können Sie die Erneuerungsfunktion im Webportal „MyServerPass“ nicht nutzen.
 Die Angaben des zu erneuernden Zertifikates lassen sich z. B. im Webportal „MyServerPass“ anschauen. Dieser Vorgang wird in der Anleitung beschrieben.
 Der Webserver läuft bis zum Import des neuen Zertifikats mit dem bestehenden Zertifikat weiter.

2.3 Erneuerung durchführen

Melden Sie sich am Kundenportal „myServerPass“ an.
 Unter dem Menüpunkt „Meine Zertifikate“ erscheint eine Liste aller Ihrer Zertifikate, siehe Abbildung 1.
 Hier können Sie nun das zu erneuernde Zertifikat anhand der Referenznummer ermitteln. ggf. lassen sich die Zertifikatseinträge durch Klicken auf die „Referenznummer“ oder den „Common Name“ anzeigen.

Abbildung 1 (Ausschnitt des Kundenportals):

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

Durch Klicken auf die Referenznummer lassen sich die Zertifikatdetails anzeigen.

Abbildung 2: (Zertifikatdetails)

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="Sperrern"/> <input type="button" value="Verlängern"/> <input type="button" value="Abbrechen"/>	

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 3.

Abbildung 3:

Angaben zum Zertifikat	
Referenznummer	220002
SubjectDN	C=DE, O=Musterorganisation, OU=Musterorganisationseinheit, ST=Bundesland, L=Musterstadt, CN=testhost.example.com
Gültig von	01.02.2013 08:50 UTC
Gültig bis	06.02.2014 23:59:59 UTC
IssuerDN	C=DE,O=T-Systems International GmbH,OU=Trust Center Services,CN=TeleSec ServerPass CA 1

Voucher-Code (Nur zum Einlösen angeben):

Daten zum Zertifikat

ROOT-Auswahl * TeleSec-CA-1

Produktauswahl * ServerPass 3 Jahre Gültigkeit
 ServerPass 2 Jahre Gültigkeit
 ServerPass 1 Jahr Gültigkeit

Preis (ohne USt.): **150,00 EUR (ohne USt.)**

Anschließend wird die Verwendung des Public Keys abgefragt, siehe Abbildung 4.

2.3.0 Die Verwendung des Public Keys bei der Erneuerung

Bei einer Erneuerung stehen zwei Optionen zur Auswahl, siehe Abbildung 4:

Abbildung 4: (Verwendung des Public Keys)

Wenn Sie einen neuen Public Key und damit einen neuen CSR für die Zertifikatserneuerung verwenden wollen, wählen Sie < Nein > und fügen Sie anschließend Ihren neuen CSR für Erneuerung in das eingblendete Feld ein.

Wichtig! Bitte beachten Sie! Es wird nur der Public Key aus dem CSR für die Zertifikatserneuerung verwendet. Eventuelle Änderungen in Ihrem neuen CSR werden ignoriert und mit dem Zertifikatsinhalt des bestehenden Zertifikats überschrieben. Falls sich der Zertifikatsinhalt geändert hat, verwenden Sie den Neuauftrag.

Wollen Sie den aktuellen Public Key wieder verwenden? *

Ja Nein (abhängig vom verwendeten Servertyp)

2.3.1 Erneuerung unter Wiederverwendung des Public Keys

Sofern der private Schlüssel des zu verlängernden Zertifikats vorhanden ist, muss nicht zwingend ein neuer Request erzeugt werden, man kann hier die Option „Ja“ auswählen und den Onlineauftrag absenden.

Er wird ein Zertifikat unter Verwendung des öffentlichen Schlüssels des zu erneuernden Zertifikats erzeugt.

2.3.2 Erneuerung unter Verwendung eines neuen Public Keys

Steht der private Schlüssel des zu verlängernden Zertifikats nicht mehr zur Verfügung, muss zunächst ein neuer Schlüssel und anschließend ein neuer Request erzeugt werden, z. B. gemäß Anleitung „Apache 2 Webserver -> Zertifikat-Requesterzeugung, Installation der Zertifikate“.

Die Feldeinträge (Common Name, Locality, Country usw.) des zu erzeugenden Request müssen exakt dem zu erneuernden Zertifikat entsprechen.

Diese Einträge lassen sich z. B. im Kundenportal „MyServerPass“ ermitteln.

Melden Sie sich am Kundenportal „myServerPass“ an.

Unter dem Menüpunkt „Meine Zertifikate“ erscheint eine Liste aller Ihrer Zertifikate, siehe Abbildung 5.

Abbildung 5: (Ausschnitt des Kundenportals):

Status:	alle (exkl. abgelaufen) ▾			Suchen			
Refnr. ▾	Typ	Neu/Ern.	CommonName	Techn. Kontakt	Ausgestellt	Ablauf	Status
220002	SSL	Neu	testhost.example.com	██████████	01.02.2013	06.02.2014	aktiv

Hier können Sie nun das zu erneuernde Zertifikat anhand der Referenznummer ermitteln. Lassen Sie sich die Zertifikatseinträge durch Klicken auf die „Referenznummer“ oder den „Common Name“ anzeigen, siehe Abbildung 6.

Abbildung 6: (Zertifikatsdetails)

Angaben zum Zertifikat	
Referenznummer	220002
SubjectDN	C=DE, O=Musterorganisation, OU=Musterorganisationseinheit, ST=Bundesland, L=Musterstadt, CN=testhost.example.com
IssuerDN	C=DE, O=T-Systems International GmbH, OU=Trust Center Services, CN=TeleSec ServerPass CA 1
Gültig von	01.02.2013 08:50 UTC
Gültig bis	06.02.2014 23:59 UTC
Status	aktiv

Die Erzeugung eines Serverschlüssels sowie eines Zertifikatsrequests wird beschrieben in der Anleitung „Apache 2 Webserver“ → „Zertifikat-Requesterzeugung, Installation der Zertifikate“.

Sobald der neue Request für die Erneuerung vorliegt, so wählen Sie bei der Frage „Wollen Sie den aktuellen Public Key wieder verwenden?“ die Option „Nein“ und kopieren den Request in das Feld **Mein PKCS#10 Zertifikats-Request** (inklusive der ----BEGIN.... und ----END... Zeilen).

Nach dem Einfügen werden die Request-Inhalte zur Kontrolle angezeigt, siehe Abbildung 7.

Abbildung 7



Prüfen Sie die angezeigten Zertifikatsdaten sowie Ihre Kontaktdaten und senden das Formular ab.

Es wird ein Zertifikat unter Verwendung der Schlüsselkennung des Public Keys des soeben eingestellten Request erzeugt. Zu Grunde gelegt werden die Zertifikatsinhalte (Common Name, Organisation usw.) des zu erneuernden Zertifikats. Eventuell anders lautende Angaben des Requests werden überschrieben.

2.4 Import des erneuerten Zertifikats

2.4.1 Herunterladen des erneuerten Zertifikats

Sie können das Zertifikat im Portal „myServerPass“ herunterladen:

www.telesec.de/serverpass/index.html (→ myServerPass)

Wählen Sie den Menüpunkt „Meine Zertifikate“

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

Abbildung 8

Status: <input type="text" value="alle (exkl. abgelaufen)"/>							<input type="button" value="Suchen"/>	
Refnr. ▼	Typ	Neu/Ern.	CommonName	Techn. Kontakt	Ausgestellt	Ablauf	Status	
220008	SSL	Ern.	testhost.example.com	[REDACTED]	01.02.2013	06.02.2014	aktiv	

Wählen Sie das herunterzuladende Zertifikat durch Klick auf die Referenznummer aus.

Abbildung 9

Angaben zum Zertifikat	
Referenznummer	220008
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 11:38 UTC
Gültig bis	06.02.2014 23:59 UTC
Status	aktiv
Auftragstyp	Erneuerung des Auftrags mit RefNum 220002
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="Sperrern"/> <input type="button" value="Verlängern"/> <input type="button" value="Abbrechen"/>	

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

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

2.4.1a 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 wird die herunter geladene Datei an die Stelle des zu erneuernden Zertifikats kopiert, die ursprüngliche Datei wird hierbei überschrieben, z. B. durch diesen Befehl: „cp /etc/apache2/servpass-123456-x509.pem /etc/apache2/ssl.crt/server.crt

Nun muss der Webserver neu gestartet werden, siehe Punkt 2.5

2.4.1b 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 10 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 10 (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-----
MIIFxiCCBK6gAwIBAgICQBMwDQYJKoZIhvcNAQEFBQAwgYlxCzAJBgNVBAYTAkRF
...
OGAb1gNE4cu5uYPKtTLbFVyaZ6EhHUoM00Vwl63IU9TUhCfrEUZUb5HI
-----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-----
lkjhgGUKjhlkLKLKKJLKhguGugtuigjkZIU
...
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-----

```

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 11.

Abbildung 11: (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 13 gezeigten Aufbau.

Abbildung 12 (ca.crt)

```

-----BEGIN CERTIFICATE-----
MIIDdTCCA12gAwIBAgILAgAAAAA1ni3l
...
X7CAuzHgC1QBXBYdck7VKmlH0Rtmfl8Bb
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDdTCCA12gAwIBAgILAgAAAAA1ni3l
...
Zg6C3ZjL2sJETy6ge/L3ayx2EYRGinij4w==
-----END CERTIFICATE-----

```

← CA Zertifikat „ServerPass CA1“

← Root Zertifikat „Baltimore Cybertrust Root CA“

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 wird 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 wie 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 das Zertifikat der ausstellenden Instanz(en), siehe Abbildung 13 bzw. 15. Jedoch wird diese Direktive von einigen älteren Server-Versionen nicht unterstützt.

Anschließend muss der Webserver neu gestartet werden, siehe 2.5

2.5 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.

2.6 Sicherung der erzeugten Dateien

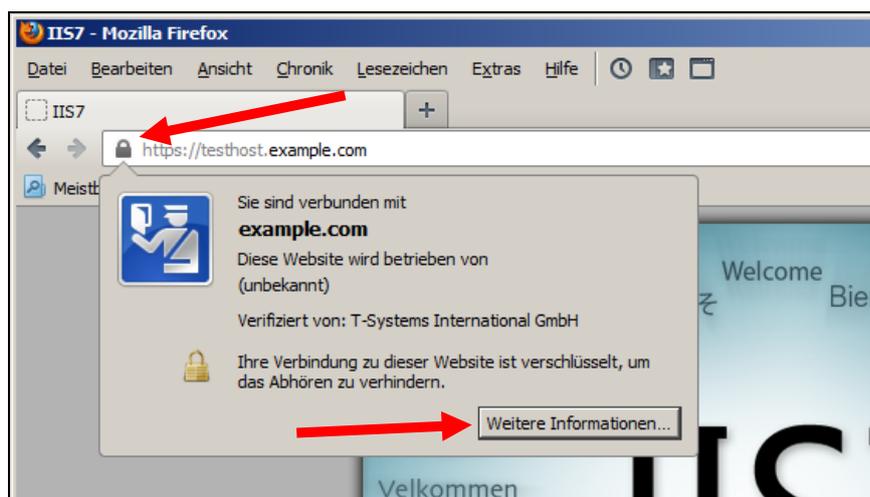
Es wird empfohlen, die erzeugten Schlüssel- und Zertifikats-Dateien zu sichern, z. B. auf einem externen Medium!

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 13-15) sowie im Internet Explorer (Abbildung 16-17) aufgeführt.

Firefox:

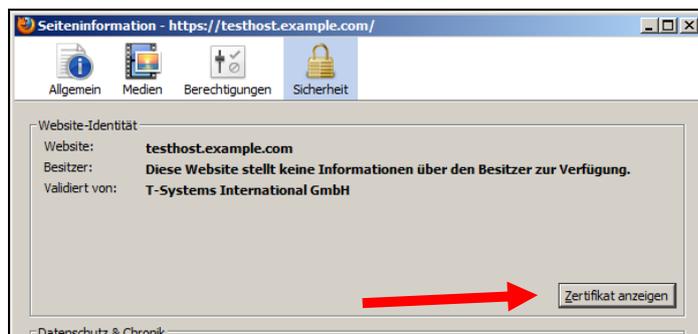
Abbildung 13 (Firefox 18):



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

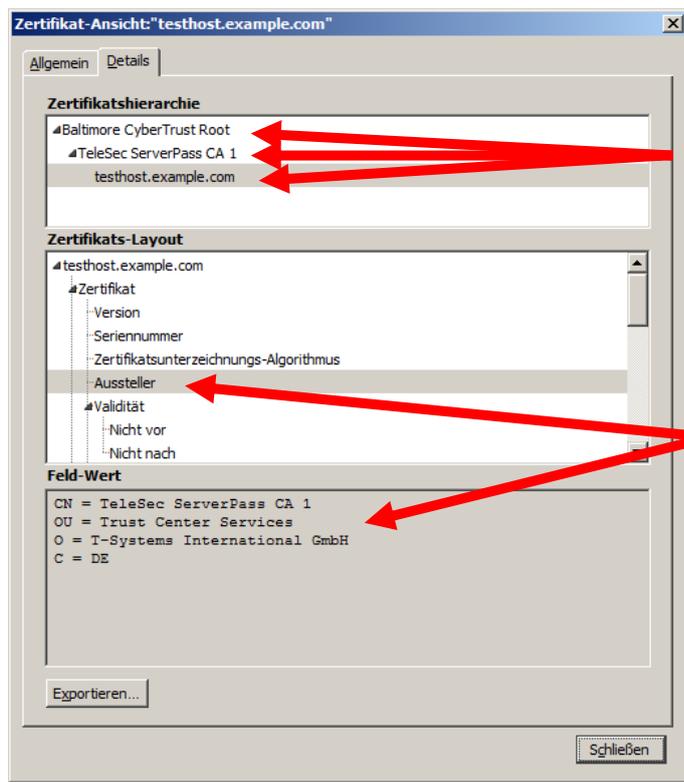
Möchten Sie weitere Informationen über das Zertifikat erfahren, so ist die über den entsprechenden Button möglich.

Abbildung 14 (Firefox 18):



Wählen Sie „Zertifikat anzeigen“.

Abbildung 15 (Firefox 18):



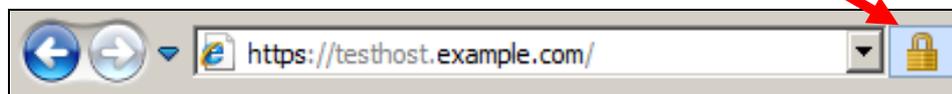
Darstellung der kompletten Zertifikatskette

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

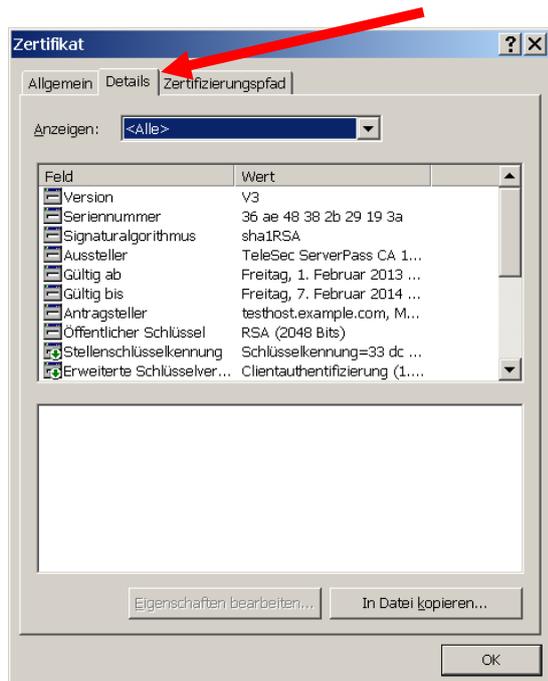
Abbildung 16 (IE 7, IE 8):



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

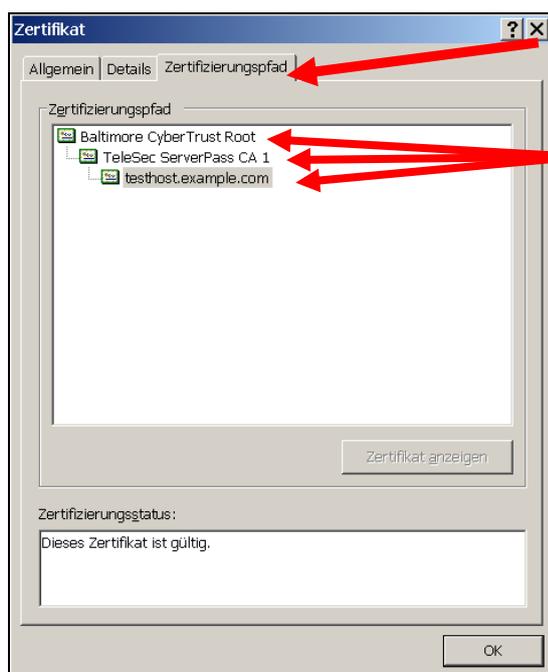
Über den Reiter „**Details**“ lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 17.

Abbildung 17 (Die Zertifikatdetails)



Über den Reiter „**Zertifizierungspfad**“ lässt sich die Zertifikatskette prüfen, siehe Abbildung 18.

Abbildung 18 (Die Zertifikatskette)



Darstellung der kompletten Zertifikatskette

So wie in Abbildung 18 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.