TeleSec ServerPass

Zertifikat-Requesterzeugung mit dem Oracle iPlanet 7 Webserver



Version: 1.1 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_oracle_iplanet_7_webs erver.doc		Requesterzeugung Oracle iPlanet 7 Webserver
Version	Stand	Status
1.1	19.02.2013	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 *	Telesec_Support@t- systems.com
	* Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute	
Kurzinfo		

Kurzinfo

Zertifikat-Requesterzeugung mit dem Oracle iPlanet 7 Webserver

T...

.

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	16.02.2013	Trust Center T-Systems, ASC	Erster Entwurf
1.0	19.02.2013	Trust Center T-Systems, ASC	Inhalt- und Layoutanpassung
1.1	10.04.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

.

1	Allgemeines	5
	1.1 Testzertifikate	6
	1.2 Spezielle Hinweise für Oracle iPlanet 7 Webserver	6
	1.2.1 Vorbereiten des Webservers	7
2	Requesterzeugung, Beauftragung, Installation, Sicherung des privaten Schlüssels	12
	2.1 Requesterzeugung	12
	2.1.1 (*) Stichwort "Common Name"	14
	1.1 Beauftragung des Serverzertifikats	17
	2.3 Herunterladen und Import der Zertifikate	18
	2.3.1 Herunterladen der Zertifikate	18
	2.3.2 Import der Zertifikate	20
	2.3.3 Prüfen, ob das Root-Zertifikat bereits im Zertifikatsspeicher des Webservers vorhanden ist	21
	2.3.5 ggf. Import des Root-Zertifikat "Baltimore CyberTrust Root"	23
	2.3.6 Import des CA-Zertifikats "TeleSec ServerPass CA 1"	26
	2.4 Installation des Serverzertifikats	28
	2.5 Sicherung der Dateien	35
3	Kontrolle	36

 \cdots T

1 Allgemeines

Dieses Dokument beschreibt die Requesterzeugung sowie die Einbindung der Zertifikate im Oracle iPlanet 7 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 Office-Paketen 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: <u>https://www.telesec.de</u> \rightarrow ServerPass \rightarrow 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: <u>https://www.telesec.de</u> \rightarrow ServerPass \rightarrow Support \rightarrow Root- / Sub-CA-Zertifikate Hier werden ebenfalls alle relevanten Details wie Serienpummer. Laufzeit Eingerprint

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 <u>einmal</u> 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 Oracle iPlanet 7 Webserver

Die Beschreibung bezieht sich auf folgende Softwarekonstellation:

Plattform: Microsoft Server 2008 R2 Oracle iPlanet 7.0 Webserver Beliebiger Internetbrowser, hier Firefox 18

Voraussetzung: Der Webserver startet bereits im unverschlüsselten Modus

Im Beispiel wird die Administration über die webbasierte "Administration Console" beschrieben.

1.2.1 Vorbereiten des Webservers

Diese Kurzanleitung dient lediglich als Installationshilfe. Es wird nicht auf die einzelnen Einstellungsmöglichkeiten des Oracle iPlanet 7 Webservers eingegangen. Weiterführende Informationen erhalten Sie in der Dokumentation des iPlanet Webservers.

Gezeigt wird hier lediglich eine Minimalkonfiguration, um den Webserver im SSL-Modus betreiben zu können

Wir gehen hier von einer Standardinstallation und einem Standardbetrieb des Webservers aus.

Das bedeutet: es wurde bereits ein betriebsfähiger Oracle iPlanet 7 Webserver installiert und nun soll zusätzlich zur Standardverbindung auch eine verschlüsselte Verbindung per SSL zum Server ermöglicht werden.

Sollten Sie die Vorbereitungen schon durchgeführt haben, so können Sie diesen Schritt überspringen.

Standardmäßig antwortet der Webserver auf Anfragen per http auf Port 80. Um zusätzlich auch verschlüsselte Anfragen zu ermöglichen, wird im Beispiel ein weiterer Virtueller Server eingerichtet, der Anfragen per https auf Port 443 entgegennimmt. Andere Vorgehensweisen sind ebenfalls möglich

Die Konfiguration geschieht über die Administration des iPlanet, siehe Abbildung 1

Knoten Allgemeine Aufgaben Konfigurationen Serverzertifikate Überwachung Allgemeine Aufgaben Klicken Sie auf die Schaltfläche "i", um weitere Informationen zu einer Aufgabe zu erhalten. Wenn Sie eine weitere Erläuterung der Terminologie wünschen klicken Sie hier Konfigurationsaufgaben Virtuelle Server-Aufgaben • i • i Konfiguration auswählen: TESTHOST Virtuellen Server auswählen: TESTHOST i i Konfiguration bearbeiten Virtuellen Server bearbeiten Webanwendung hinzufügen Neue Instanz i i Dokumentverzeichnisse Instanzen starten/anhalten i i CGI-Verzeichnisse Java-Einstellungen bearbeiten i i Protokolleinstellungen und Archivierung i URL-Umleitungen i i Serverzertifikat anfordern i Umgekehrter Proxy einrichten Serverzertifikat installieren i Zusammenfassung anzeigen i Zusammenfassung anzeigen i i Neuer virtueller Server Neue Konfiguration i 6.0/6.1-Instanzen migrieren i i Protokolle anzeigen

Nach der Anmeldung an der "Administration Console" stehen alle Konfigurationsaufgaben zur Auswahl bereit.

Wählen Sie den Reiter "Allgemeine Aufgaben" und unter dem Menü "Virtuelle Server-Aufgaben" den Punkt "Neuer virtueller Server".

Abbildung 1

Assistent	für neu	en virtue	llen Server	
Schritte	Hilfe		Schritt 1:Konfiguration auswählen	
⇒ 1. Konfigura	ation aus	wählen	Wählen Sie die erforderliche virtuelle Serverkonfiguration.	
 Informativituellen HTTP-Lis [Schrift w Auswahl Schrift be 	onen zum Server ei istener aus ird durch i im vorher stimmt]	ngeben swählen die igen	* steht für Pflichtfelder * Konfiguration auswählen IESTHOST Wählen Sie eine Konfiguration aus der oben angezeigten Liste.	prechen

Wählen Sie die gewünschte Konfiguration aus und klicken auf "Weiter".

Abbildung 3

Assistent für neuen virtuellen Server									
Schritte H	ilfe	Schritt 2:Informat	Schritt 2:Informationen zum virtuellen Server eingeben						
1. Konfiguration	1 auswählen	Geben Sie einen Nam Server ein.	Geben Sie einen Namen und optional eine Beschreibung für den neuen virtuellen Server ein.						
 2. Informatione virtuellen Se eingeben 	en zum rver		* steht für Pflichtfelder						
3. HTTP-Listen	er auswählen	* Name:	TESTHOST-SSL Der Name kann alphanumerische Zeichen sowie Punkte (.), Striche (-) und Unterstriche (-) enthalten.						
[Schritt wird o Auswahl im v Schritt bestin	durch die vorherigen nmt]	Hosts:	TESTHOST Sie können mehrere URL-Hosts, getrennt durch Kommas, eingeben.						
		Dokument-Root:	C:\iPlanet-SSL Dokument-Root-Verzeichnis						
		Zurück Weiter	Abbrechen						

Vergeben Sie einen Namen für den neuen virtuellen Server sowie den Pfad zu den Webdokumenten (Dokument-Root).



In der nächsten Abbildung wird die Erstellung eines neuen http-Listeners angestoßen. Hierin wird u. a. der Port für die SSL-Verbindungen festgelegt, siehe Abbildung 5.

Abbildung 5

Assistent für neuen virtuel	Assistent für neuen virtuellen Server										
Schritte Hilfe	Geben Sie zum Erstellen ei Portnummer ein.	nes neuen H I I P-LISTENERS einen Mamen und eine									
1. Konfiguration auswählen		* steht für Pflichtfelder									
2. Informationen zum virtuellen Server eingeben	* Name:	http-listener-ssl Name, der den HTTP-Listener eindeutig identifiziert									
3. HTTP-Listener auswählen	* Port:	443 Port, auf dem überwacht wird									
 3.1 Neuer HTTP-Listener 	* IP-Adresse:	* IP-Adresse oder * zur Überwachung auf allen									
4. Überprüfen der Einstellungen	* Servername:	TESTHOST Name des Standardservers									
5. Ergebnisse	* Standardmäßiger virtueller Server:	TESTHOST-SSL Name des virtuellen Servers zur Verarbeitung von Anforderungen, für die kein Host gefunden wurde									
	Zurück Weiter	Abbrechen									

Für den neuen HTTP-Listener können die Angaben gemäß Abbildung 5 festgelegt werden. Standardmäßig wird dieser Port verwendet: **443**.

Falls der Bereich für SSL erscheinen sollte, der "SSL-Modus" wird hier noch nicht aktiviert.

Schritte	Hilfe		Schritt 4:Überprüfen der Einstellungen					
1. Konfiguration auswählen			Prüfen Sie hier Ihre Einstellungen. Klicken Sie auf 'Fertig stellen', um den Vorgang fortzusetzen.					
virtuelle	n Server ei	ngeben						
3 HTTPJ	istanar aus	wählen	Name des virtuellen Servers:	TESTHOST-SSL				
5. IIIII - E	isterier aus	wanten	Hosts:	TESTHOST				
3.1 Neuer HTTP-Listener		Listener	Dokument-Root:	C:\iPlanet-SSL				
4 Übornri	ifon dor		Ausgewählte Listener:	Keine				
Einstell	ungen		Neuer Listener					
			Name: http-listener-s	sl				
5. Ergebni	sse		Port: 443					
			Zuzüele Eestis stelles	Abbrahan				

Gemäß Abbildung 6 lassen sich die Einstellungen überprüfen und "Fertig stellen".

Abbildung 7



Der neue virtuelle Server wurde erfolgreich angelegt.

Abbildung 8

VERSION						STARTSEITE	AKTUALISIEREN	ABMELDEN	HILFE			
Benutzer: admir	Server: TESTHOST					A Bere	itstellung steht a	<u>BUS</u>	Ľ,			
Instanz(en) wurden angehalten $①$ 0 Java												
Konfigurationen	> TESTHOST											
Virtuelle Server	HTTP-Listener	Instanzen	Allgemein	Leistung	Zugriffssteuerung	Zertifikat	e Java	Zusammenfa	issung			
TESTHOST Mit virtuellen Se nur einen instal Hardwarewartu Server erstellen	- Virtuelle Server of vern können Sie mehrere erten Server besitzen. Fü g und die grundlegende und bearbeiten.	der Konfigu en Firmen oder r die Benutzer Webserververv	Jration Personen Domä wirkt es fast so, a valtung übernehn	nennamen, Is ob sie ül nen. Auf die	IP-Adressen und einige (er einen eigenen Webse ser Seite können Sie die (Serverüberwacl rver verfügen w für eine ausgev	nungsfunktioner ürden, wennglei vählte Konfigura	n anbieten, müss ich Sie die tion definierten v	en aber irtuellen			
Virtuelle S	rver (2)	_	_	_	_	_	_	_				
Neu D	Iplizieren Webanwe	endung hinzufü	igen Lösch	en								
≶ B Name		▲ List	tener		Hosts	Dokume	nt-Root					
TEST	HOST	[*:8	0]		TESTHOST	c:\iPlane	t					
TEST	HOST-SSL	[*:44	43]		TESTHOST	C:\iPlan	et-SSL					

11 • •

.



In der Konfiguration wird nun der neue virtuelle Server aufgelistet. Die Änderungen müssen über den Link "**Bereitstellung steht aus**" aktiviert werden.

Abbildung 9

Konfigur Bereitsteller	rationsbereitstellung n einer Konfiguration für alle Instanzen	
	Bereitstellung steht aus Die Konfiguration TESTHOST wurde lokal geändert. Klicken Sie auf "Bereitstellen", um die Änderungen für alle Instanzen zu übernehmen.	
	Bereitstellen A	bbrechen

Über "Bereitstellen..." werden die Änderungen übernommen.

Abbildung 10

Instanzen erfordern einen Neustart testhost ADMIN3594: Änderungen an der Konfiguration erfordern einen Neustart des Servers.								
Instanzen neu starten:	 Jetzt 	C Später						
			OK Schli					

Damit die Änderungen wirksam werden, müssen die Instanzen neu gestartet werden.

<u>Abbildung 11</u>

Instanz(en) wurde(n) erfolgreich neu gestartet

Der erfolgreiche Neustart wird entsprechend quittiert.

Die Vorbereitung ist hiermit abgeschlossen und die Requesterzeugung kann beginnen.

2 Requesterzeugung, Beauftragung, Installation, Sicherung des privaten Schlüssels

2.1 Requesterzeugung

In dieser Anleitung wird kein Passwort zum Schutz der Zertifikate vergeben. Wenn gewünscht, kann über den Reiter "PKCS11-Token" ein Passwort definiert werden. Wurde ein Passwort definiert, so muss es bei den nachfolgenden Aktionen immer wieder eingegeben werden.

Abbildung 12

Konfigurationen > TESTHOST											
Virtuelle Server	HTTP-Listener		P-Listener Instanzer		Allgemein	Lei	stung	Zugriffssteuerung		Zertifikate	Java
Serverzertifi	ikate	Zertifikatau	ssteller	CF	RL-Aktualisierur	ngen	PKC	PKCS11-Token			
TESTHOST - Konfiguration von Serverzertifikaten Passwörter festlegen Zertifikate bestehen aus digitalen Daten, die den Namen einer Person, einer Firma oder einer anderen Entität angeben und bescheinigen, dass der im Zertifikat enthaltene öffentliche Schlüssel dieser Entität gehört. SSL-aktivierte Server müssen ein Zertifikat besitzen, für Clients ist das Zertifikat optional. Auf dieser Seite können Sie Serverzertifikate anfordern, installieren, erneuern und löschen.											
Serverzei	rtifika	te (0)	_	-	_			_	_	_	
Anforderun	Anforderung Installation Erneuern Löschen Filter: Alle Elemente										
Pseudonym			Ausst	teller			Token		Ablaufdatu	m	
Keine Zertifikate gefunden. Einige Zeilen dieser Tabelle sind möglicherweise ausgeblendet, da ein Filter angewendet wurde. Wählen Sie die Einstellung "An Elemente" in der Filterliste, um alle Zeilen anzuzeigen.											

Nun wird die Requesterzeugung angestoßen.

Dies geschieht im Reiter "Serverzertifikate" über "Anforderung..."

Assistent für Serverzertifikatanf	orderung
Schritte Hilfe	Schritt 1: Token und Passwörter auswählen
 1. Token und Passwörter auswählen 	Die Seite zeigt die Liste mit den für die Konfiguration verfügbaren Token. Geben Sie das Passwort für das ausgewählte Token ein, sofern erforderlich.
2. Serverdetails eingeben	
3. Zertifikatoptionen	Konfiguration: TESTHOST
4. Zertifikatstyp	Token: Internal 💌
5. Überprüfen der Einstellungen	Wählen Sie den Tokennamen aus der obigen Liste. Wenn ihr Schlüssel in der Nokalen, von Oracle iPlanet Web Server verwalteten Schlüsseldatenbank gespeichert ist, wählen Sie Intern', Wenn ihr Schlüssel auf einer Smartcard oder auf einem anderen externen Gerät
6. Ergebnisse	gespeichert ist, wählen Sie den Namen des externen Tokens aus dem Dropdown-Listen feld.
	Geben Sie das Passwort für das ausgewählte Token ein. Das Passwortfeld ist nur dann aktiviert, wenn das ausgewählte Token ein Passwort erfordert.
	Zurück Weiter Abbrechen

Es öffnet sich der Assistent für die Serverzertifikatinstallation.

Wählen Sie unter Token "Internal" aus und tragen ggf. Ihr zuvor definiertes Passwort ein.

Abbildung 15

Assistent für Serverzertifikatanforderung							
Schritte Hilfe	Schritt 2:Serverdetails	eingeben					
1. Token und Passwörter auswählen	Geben Sie die Informationen zum Generieren der Zertifikatanforderung ein.						
➡ 2. Serverdetails eingeben		* steht für Pflichtfelder					
3. Zertifikatoptionen	* Servername:	testhost.example.com Dies kann ein einzelner Servername, z. B. www.sun.com, oder eine mit Kommas getrennte Liste von Servernamen sein, z. B. www.sun.com,java.sun.com					
4. Zertifikatstyp							
5. Überprüfen der Einstellungen	Organisation (o):	Musterorganisation					
6. Ergebnisse	Organisationseinheit (ou):	Musterorganisationseinheit					
	Ort (I):	Musterstadt					
	Bundesland (st):	Bundesland					
	Land/Region (c):	Deutschland DE					
		Wählen Sie das Land, oder geben Sie den zweistelligen Ländercode ein.					
	Zurück Weiter	Abbrechen					

Nun werden die einzelnen Zertifikatseinträge festgelegt, diese Angaben erscheinen später unverändert im Zertifikat, im Einzelnen sind dies die folgenden Einträge.

.

Beschreibung der Zertifikatseinträge:

"Gemeinsamer Name" Hier "Servername"	(*, 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 Organisations- einheit, 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 (**C**ertificate **P**ractice **S**tatement) aufgeführten Hinweise. Insbesondere den erlaubten Zeichensatz. Siehe hierzu: www.t-systems-telesec.com (\rightarrow Online Auftrag \rightarrow Telekom Zertifikate)

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

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 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.

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).

Nachdem alle Angaben gemacht wurden, gelangen Sie über den Button "**Weiter**" zu Abbildung 16.

Assistent für Serverzertifikata	anforderung
Schritte Hilfe	Schritt 3:Zertifikatoptionen
1. Token und Passwörter auswählen	Geben Sie den Schlüssellyp für das Zertifikat an.
2. Serverdetails eingeben	Schlüsseltyp
3. Zertifikatoptionen	© RSA
4. Zertifikatstyp	Schlüsselgröße: 2048 V Bit
5. Überprüfen der Einstellungen	C ECC 406
6. Ergebnisse	Kurvenname: prime256v1
	•
	Zurück Weiter Abbrechen

Unter "Schlüsseltyp" muss der Typ "**RS**A" ausgewählt werden sowie unter Schlüsselgröße ein Wert von 2048 Bit.

Dies ist der Wert für die Schlüssellänge des Server-Keys und der späteren Zertifikate. Mögliche Werte sind:

2048 oder 4096.

Empfohlen wird eine Bitlänge von 2048, <u>maximal</u> jedoch 4096 Bit. Requests mit einer Bitlänge kleiner 2048 Bit gelten nicht länger als sicher

und sind von der Beauftragung ausgeschlossen

Abbildung 17

Token und Passwörter auswählen Serverdetails eingeben Zertifikatoptionen Zertifikatstyp Überprüfen der Einstellungen Ergebnisse	Wählen Sie die Zertifikatsignaturstelle (Certificate Signing Authority, CSA) für das Zertifikat * Selbst signiertes Zertifikat * Pseudonym: Gültigkeitsdauer: Listener:KEINER
-	C ZA-signiertes Zertifikat

In Abbildung 17 wählen Sie "ZA-signiertes Zertifikat"

· · · ·

. . .

Assistent für Se	Assistent für Serverzertifikatanforderung							
Schritte Hilfe		Schritt 5:Überprüfen der Ein	stellungen					
1. Token und Passwörter auswählen		Prüfen Sie hier Ihre Einstellungen. Klicken Sie auf 'Fertig stellen', um den Vorgang fortzusetzen.						
2. Serverdetails eingeben		Konfiguration: TESTHOST						
3. Zertifikatoptione	n	Token: internal						
4. Zertifikatstyp		Serverdetails Servername:	testhost.example.com					
➡ 5. Überprüfen der Einstellungen		Organisation (o):	Musterorganisation					
6. Ergebnisse		Organisationseinheit (ou): Ort (I): Bundesland (st): Land/Region (c): Zertifikatstyp Typ: ZA-signiert Zertifikatoptionen Schlüsseltyp: RSA Schlüsselgröße: 2048	Musterorganisationseinheit Musterstadt Bundesland DE					
		Zurück Fertig stellen	Abbrechen					

Sind alle Angaben korrekt, kann der Request über "Fertig stellen" erzeugt werden.

Abbildung 19

Assistent für	erv	erzertifikatanf	orderu	ung
Schritte Hil	•		Schr	itt 6:Ergebnisse
 Token und Pa auswählen Serverdetails Zertifikatoptio Zertifikatstyp Überprüfen d Ergebnisse 	sswö einge en r Ein	rter :ben stellungen		Certifikatsignaturanforderung (CSR) Filder CSA Comparison of the CERTIFICATE REQUEST MIDINTOCAAAOCAQAwgZUXC2AJBgNVBAYTAKREMRMwEQDIVQQIEwpCdWSkZXNaYWSk MRwEgYDVQQHEwtNdXNOZXJzdGFkdDEZMBoGAIUEChMQVGVZdG9y22FuaXNhdGlv bjEhuB8GAIUECxMYVGVZdG9y22FuaXNhdGlvbnllaW5oZNIOMR0wGWJDVQQDExR0 ZXN0aG9zdC51eGFtoGx1LmNvbICCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC gdEBAMPIHSIopg614aoXhmfjp9FTDUgPTI8dUWIIXtpINM/m3SSW/XpcDWw6hmWE S/QJW9UF2+EjH7A9AhLBj/cDE2ITURK+iDPjYItaxSEXvbwrnw6wX0Kiec02jo6X VomE9M6aNyC/SYW7kZVIUqMGnEmz8DNkaoQ3LCLKuhIEiKhIHQirpETyjmbRh7Uq wcCfenUeAEU9xAVAkG7AloaejditIVXrXuzq+ICSgAuC+GRWNHWU6JZDgPSZuMi uhqPWbunx9DSp4Tno8vgw82jAdhIwUivXmJP4jODIIAmU59nitA6TzmtoUM3ImFa PZV8hqQ5GgobotuxmB+d8gskSUCAwEAABBMFgGCSqSIB3DQEJDjFLMEkwHwDi UndDExribeUHdULAChurgeVYbbVD2ZEEbb0AU-WUMDUADU AburceVIIMU

Der Request wurde erzeugt. Bitte kopieren Sie ihn aus dem Feld unter "Zertifikatsignaturanforderung (CSR)" incl. der "----BEGIN.... und ----END... " Zeilen per cut & paste in eine eigene Datei, z. B. zertifikat-requestdatei.txt. Alternativ lässt sich der Request auch direkt in das entsprechende Feld im Onlineauftrag kopieren.

. . .



Abbildung 20 (zertifikat-request.txt)

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBxzCCAtrrtTACAQAwgYYxCzAJBgNVBAYTAkRFMQwwCgYDVQQIEANBgNV
```

DGysW9I7Wv9SOeW5HrhL4SIlzVVVzFUW5NvRpQCaE+qIkpo+w9l5K0/HFn5mWSkT cPMXx5uYkJNO8l9REmvcJMhvJIzw4vP+kyjM -----END NEW CERTIFICATE REQUEST-----

1.1 Beauftragung des Serverzertifikats

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

<u>https://www.telesec.de/serverpass/</u> (-> 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 20, inklusive der "----BEGIN.... und ----END... " Zeilen per cut & paste.

Nach dem Einfügen werden die Request-Inhalte zur Kontrolle angezeigt, siehe Abbildung 21.

Bitte überprüfen Sie nach dem Einfügen des Requests die angezeigten Inhalte.						
Mein PKCS#10 Zertifikats-Request *						
AjALBgIghkgBZQMEAQUwBwYFKw4DAgowCgYIKoZIhvcNAwcwHQYDVR0OBBYEFGCn BZgKDIBRRd5RDtejtu8UVri1MA0GCSqGSIb3DQEBBQUAA4IBAQDRRifAlKxLmH8r hXFXNtgF33ABSq4OcmTNWMhle+f1wHQ9D2TuJKt2v4LVET8WCtkF23E9XI9OO9gb nXQf9VWHfnbqbOsD/7AKnno9X9TmEzA7mkGe4khRH8vccPeTP+aDFuA5r8ojT95p mxkIJ7qsvSQ17QI/mEDc5xL6/AZ/DUKI2s28uQjV4gIfd/zd8a0GrgyHzE+ztJ3 ZZDJiqsOYJWpwWq0vpBXmP7I1RnJ+b3jNBfYf2xyiaI9umMDYbyMjoSTY7xve42D wCKGkw/OD8YhUoQsQTW1fkwVBM1kUz4rqYiIA+cE2/510S1JvMYPIT0JU/cmn4IV sMp1uF/2 END NEW CERTIFICATE REQUEST						
Ihr Zertifikats-Requ	est wurde untersucht und enthält den nachfolgenden Inhalt:					
CN:	testhost.example.com					
C:	DE					
0:	Musterorganisation					
OU1:	Musterorganisationseinheit					
ST:	Bundesland					
L:	Musterstadt					
SAN 1(=CN):	testhost.example.com					

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

Wählen Sie den Menüpunkt "Meine Zertifikate"

Hier werden nun alle Ihre Zertifikate aufgelistet.



Abbildung 22:

Zum Sortieren der Übersicht klicken Sie bitte in die jeweilige Spaltenüberschrift.							
Status: alle (exkl. abgelaufen) -							Suchen
Refnr.▼	Тур	Neu/Ern.	CommonName	Techn. Kontakt	Ausgestellt	Ablauf	Status
220002	SSL	Neu	testhost.example.com		01.02.2013	06.02.2014	aktiv

Wählen Sie das herunter zuladende Zertifikat durch Klick auf die Referenznummer aus, siehe Abbildung 22.

Abbildung 23

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					
Kaufm. Kontakt					
Download des BASE64 kodierten Zertifikates inkl. der kompletten Zertifikatskette.					
Download (nur Zertifikat) Download (inkl. Zertifikatskette) Sperren Verlängern Abbrechen					

Es werden zwei Download-Formate angeboten, siehe Abbildung 23:

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

Wählen Sie das Format: "Download inkl. Zertifikatskette". Aktivieren Sie die Option "Als Datei speichern und legen einen Dateipfad fest, z. B. c:\

Sie erhalten die Datei "servpass-123456-x509chain.pem" und sie liegt nun in diesem Verzeichnis: c:\ servpass-123456-x509chain.pem

2.3.2 Import der Zertifikate

Öffnen Sie die herunter geladene Datei mit einem einfachen Texteditor z. B. WordPad, ggf. muss bei Öffnen der Dateityp "Alle Dokument *.*" eingestellt werden.

So wie in Abbildung 24 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 24 (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.: UXU/2/42c2
BEGIN CERTIFICATE
 90u0NM/anP8/AdF176ziGwdUnRzL108eA
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

2.3.3 Prüfen, ob das Root-Zertifikat bereits im Zertifikatsspeicher des Webservers vorhanden ist

Zur Überprüfung öffnen Sie die Zertifikatsverwaltung, siehe Abbildung 26

. . . .

Abbildung 26

Konfiguration	Konfigurationen > TESTHOST								
Virtuelle Server	HTTP-Listener	Instanzen	Allgemein	Allgemein Leistung Zugriffssteuerung Z		Zertifikate	Java		
Serverzertif	Serverzertifikate Zertifikataussteller CRL-Aktualisierungen PKCS11-Token								
TESTHOST - Zertifikataussteller (ZAs) Passwörter festlegen Die Seite listet die verschiedenen Zertifikataussteller auf, die in der Zertifikatdatenbank verfügbar sind. Sie haben auf dieser Seite die Möglichkeit, ein ZA-Zertifikat oder eine Zertifikatsperrliste (Certificate Revocation List, CRL) zu installieren, oder Sie können ein ZA-Zertifikat löschen. Der Filter in der Tabelle kann dazu verwendet werden, abgelaufene Zertifikate anzuzeigen oder integrierte Zertifikate auszublenden.									
Zertifikataussteller (1 - 20 von 157)									
Installation	Installation CRL wird installiert Löschen Filter: Alle Elemente								
Ø₿ Pse	udonym			_	Abla	ufdatum		△ CRL	
Builtin Object Token:Baltimore CyberTrust Root 13. Mai 2025 01:59:00 MESZ Nicht installiert									
	Image: Seite: 1 von 8 Gehe zu Image: Seite: Ima								

So wie in Abbildung 26 dargestellt, muss das Zertifikat "Baltimore CyberTrustRoot" aufgeführt sein. Klicken Sie auf das Zertifikat, um sich die Details anzeigen zu lassen, siehe Abbildung 27.

412

.

. .

Z	ertifikatausst	Übernehmen	Schließen						
Di	ese Seite listet d	ie Eigenschaften des Zertifikats auf.							
A	llgemein								
	Zertifikatdetails	5							
	Pseudonym	Builtin Object Token:Baltimore CyberTrust Root							
	Betreff	CN=Baltimore CyberTrust Root,OU=CyberTrust,O=Baltimore,C=IE							
	Aussteller	CN=Baltimore CyberTrust Root,OU=CyberTrust,O=Baltimore,C=IE							
	Gültig ab	12. Mai 2000 20:46:00 MESZ							
	Gültig bis	13. Mai 2025 01:59:00 MESZ							
	Fingerabdruck	AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:	E4						
	Seriennummer	02:00:00:B9							
V	Vertrauensstufen								
	Vertrauenswürd	lig zur Signierung von Clientzertifikaten: 🛛 🗖 Ak	tiviert						
	Vertrauenswürd	lig zur Signierung von Serverzertifikaten: 🔽 Ak	tiviert						

. . .

Vergleichen Sie die Zertifikatdetails mit den Einträgen auf unserer Internetseite:

http://www.telesec.de/serverpass/support_rootca_akzeptanz.html -> "Root-CA Zertifikate"

Dieses Zertifikat ist i.d.R. in der Default-Konfiguration enthalten. Wird das Root-Zertifikat nicht aufgeführt, so importieren Sie es gemäß Punkt 2.3.5

.

2.3.5 ggf. Import des Root-Zertifikat "Baltimore CyberTrust Root"

. . .

. . .

Wählen Sie im Konfigurationsmenü wieder den Reiter "**Zertifikate**" gemäß Abbildung 26, anschließend der Reiter "**Zertifikataussteller**" und den Punkt "**Installation**", siehe Abbildung 28.

Abbildung 28

Konfigurationen > TESTHOST											
Virtuelle Server	irtuelle Berver HTTP-Listener		Instanz	nzen Allgemein Leistun		tung	Zugriffssteuerung		Zertifikate	Java	
Serverzertifikate Zertifikataussteller CRL-Aktualisierungen PKCS11-Token							S11-Token				
TESTHOST - Zertifikataussteller (ZAs) Die Seite listet die verschiedenen Zertifikataussteller auf, die in der Zertifikatdatenbank verfügbar sind. Sie haben auf dieser Seite die Möglichkeit, ein ZA-Zertifikat oder eine Zertifikatsperrliste (Certificate Revocation List, CRL) zu installieren, oder Sie können ein ZA-Zertifikat löschen. Der Filter in der Tabelle kann dazu verwendet werden, abgelaufene Zertifikate anzuzeigen oder integrierte Zertifikate auszublenden.											
Zertifikataussteller (1 - 20 von 157)											
Installation		CRL wird inst	alliert	Lös	chen Filte	r: Alle	Elemen	te	•	🗗	
≶ ⊞ Pse	udonyn	n				4	Abla	ufdatum		△ CRL	

Abbildung 29

Assistent für ZA-Zertifikatins	stallation							
Schritte Hilfe	Schritt 1: Token und Passwörter auswählen							
 1. Token und Passwörter auswählen 	Die Seite zeigt die Liste mit den für die Konfiguration verfügbaren Token. Geben Sie das Passwort für das ausgewählte Token ein, sofern erforderlich.							
2. Eingabe der Zertifikatdaten								
3. Zertifikatdetails	Konfiguration: TESTHOST							
4. Überprüfen der Einstellungen 5. Ergebnisse	Token: Internal Wählen Sie den Tokennamen aus der obigen Liste. Wenn Ihr Schlüssel in der lokalen, von Oracle iPlanet Web Server verwalteten Schlüsseldatenbank gespeichert ist, wählen Sie Intern". Wenn Ihr Schlüssel auf einer Smartcard oder auf einem anderen externen Gerät gespeichert ist, wählen Sie den Namen des externen Tokens aus dem Dropdown-Listenfeld. Passwort:							
	Zurück Weiter Abbrechen							

Es öffnet sich der Assistent für ZA-Zertifikatinstallation. Hier wählen Sie den Token "**internal**", ggf. ist die Eingabe Ihres Passworts erforderlich. . .

Schritte Hilfe	Schritt 2:Eingabe der Zertifikatdaten
1. Token und Passwörter auswählen	Geben Sie Zertifikatdaten im ASCII-Format zusammen mit den Headern im Textbereich ein, ode geben Sie den Pfad zu einer Datei an, welche die Zertifikatdaten enthält.
2. Eingabe der Zertifikatda	1
3. Zertifikatstyp	O Zertifikatdaten
4. Überprüfen der Einstellur	BEGIN CERTIFICATE MIIDdzCCAI+g&wIBAgIEAgAAuTANBgkqhkiG9w0BAQUFADB Q/1/16eYS9HRCwBXbsdtTLS MIIDdzCCAI+g&wIBAgIEAgAAuTANBgkqhkiG9w0BAQUFADB
o. Ergebnisse	Q/1/I6eYs9HRCwBXbsdtTLS /CG9VwcPCPW12yejloqhqdNkNwnGjkCAwEAAaNFMEMwHQ YDVR00BBYEFOWdWTCCR1jMrPoIVDaGezq1BE3wMBiGA1U dEwEBwQIMAYBAf8CAQMwDgYDVR0PAQH /BAQDAgEGR9I4LID+gdwyah617jz/V0eBHRnDJELqYzm FDICERTEICATF
	⊖ Zertifikatsdatei
	Pfad zur Zertifikatdatei auf dem Server
	Zurück Waiter

. . . .

In das Feld "Zertifikatdaten" kopieren Sie das das Root-Zertifikat "BaltimoreCyberTrustRootCA" incl. der ---BEGIN... und ---END... Zeilen (grün markiert) aus Abbildung 24.

Abbildung 31

Assistent für ZA-Zertifikatins	Assistent für ZA-Zertifikatinstallation								
Schritte Hilfe	Schritt 3:Zertifikatstyp								
1. Token und Passwörter auswählen	Wählen Sie den Typ des zu installierenden Zertifikats aus.								
 2. Eingabe der Zertifikatdaten 3. Zertifikatstyp 4. Überprüfen der Einstellungen 5. Ergebnisse 	Zertifikatstyp © ZA-Zertifikat C Zertifikatkette								
	Zurück	Abbrechen							

Als Zertifikattyp wählen Sie "ZA-Zertifikat".

. .

.

Assistent für ZA-Zertifikatinstallation										
Schritte Hilfe	Schritt 4:Überprüfen der Einstellungen									
1. Token und Passwörter auswählen	Prüfen Sie hier Ihre Einstellungen. Klicken Sie auf 'Fertig stellen', um den Vorgang fortzusetzen.									
2. Eingabe der Zertifikatdaten	Konfiguration: TESTHOST									
3. Zertifikatstyp	Token: internal									
➔ 4. Überprüfen der Einstellungen	Zertifikatstyp: ZA-Zertifikat									
5 Ergebnisse	Betreff: CN=Baltimore CyberTrust Root,OU=CyberTrust,O=Baltimore,C=IE									
S. Elgebhold	Aussteller: CN=Baltimore CyberTrust Root,OU=CyberTrust,O=Baltimore,C=IE									
	Schlüsseltyp: RSA									
	Schlüsselgröße: 2048									
	Gültig ab: Fri May 12 20:46:00 CEST 2000									
	Gültig bis: Tue May 13 01:59:00 CEST 2025									
	Seriennummer: 02:00:00:B9									
	Fingerabdruck: AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4									
	Zurück Fertig stellen Abbrechen									

In Abbildung 32 werden alle Details des zu importierenden Zertifikats angegeben. Vergleichen Sie die Details mit den Einträgen auf unserer Internetseite:

<u>https://www.telesec.de/serverpass/</u> -> Support -> Root-/Sub-CA Zertifikate

Über "Fertig stellen" wird der Import abgeschlossen.

Abbildung 33



Der erfolgreiche Import wird entsprechend quittiert.

Das Root-CA-Zertifikat wird nun entsprechend Abbildung 26 und 27 aufgelistet

2.3.6 Import des CA-Zertifikats "TeleSec ServerPass CA 1"

.

Wählen Sie im Konfigurationsmenü wieder den Reiter "**Zertifikate**" gemäß Abbildung 26, anschließend der Reiter "**Zertifikataussteller**" und den Punkt "**Installieren**", siehe Abbildung 28.

Abbildung 34

Assistent für ZA-Zertifikatinstal	lation						
Schritte Hilfe	Schritt 1:Token und Passwörter auswählen						
 1. Token und Passwörter auswählen 	Die Seite zeigt die Liste mit den für die Konfiguration verfügbaren Token. Geben Sie das Passwort für das ausgewählte Token ein, sofern erforderlich.						
2. Eingabe der Zertifikatdaten							
3. Zertifikatdetails	Konfiguration: TESTHOST						
4. Überprüfen der Einstellungen 5. Ergebnisse	Token: internal I Wählen Sie den Tokennamen aus der obigen Liste. Wenn Ihr Schlüssel in der lokalen, von Oracie IPlanet Web Server verwalteten Schlüsseldatenbank gespeichert ist, wählen Sie 'intern'. Wenn Ihr Schlüssel auf einer Smartcard oder auf einem anderen externen Gerät gespeichert ist, wählen Sie den Namen des externen Tokens aus dem Dropdown-Listenfeld. Passwort:						
	Zurück Weiter Abbrechen						

Es öffnet sich der Assistent für ZA-Zertifikatinstallation. Hier wählen Sie den Token "**internal**", ggf. ist die Eingabe Ihres Passworts erforderlich.

Abbildung 35

Assistent für ZA-Zertifikatins	tallation							
Schritte Hilfe	Schritt 2:Eingabe der Zertifikatdaten							
 Token und Passwörter auswählen 2. Eingabe der Zertifikatdaten 	Geben Sie Zertifikatdaten im ASCII-Format zusammen mit den Headern im Textbereich ein, oder geben Sie den Pfad zu einer Datei an, welche die Zertifikatdaten enthält.							
3. Zertifikatstyp 4. Überprüfen der Einstellungen 5. Ergebnisse	C Zertifikatdaten MIDdxCCA+qAwlBAglEAgAAuTANBgkqhkiG9w0BAQUFADB Q/I/li64'99HRCWBXbadTANBgkqhkiG9w0BAQUFADB Q/I/li64'99HRCWBXbadTANBgkqhkiG9w0BAQUFADB Q/I/li64'99HRCWBXbadTLS VID09WCPCHv112yajl00pqdhk1wnGjkCAwEAAaNFMEHwHQ YDVR00BBYEFOW/dWTCCR1jMF0vIDaGezq1BE3wMBIGA1U dewEBw2IMAYB4BCAQMwDg7DVR0PAQH I/BAQDAgECR94LD+gdwyah617/2V/0eBHRnDJELqYzm END CERTIFICATE C Zertifikatdatei Pfad zur Zertifikatdatei auf dem Server							
	Zurück Weiter Abbrechen							

In das Feld "Zertifikatdaten" kopieren Sie das das CA-Zertifikat

.

"TeleSec ServerPass CA 1" incl. der ---BEGIN... und ---END... Zeilen (magenta markiert) aus Abbildung 24.

Abbildung 36

Assistent f	Assistent für ZA-Zertifikatinstallation									
Schritte	Hilfe		Schritt 3:Zertifikatstyp							
1. Token un auswähle	d Passwö en	irter	Wählen Sie den Typ des zu installierenden Zertifikats aus.							
 2. Eingabe (3. Zertifikat 4. Überprüfe 5. Ergebnis: 	der Zertifil styp en der Ein se	katdaten Istellungen	Zertifikatstyp OZ-Zertifikat C Zertifikatkette							
			Zurück Weiter	Abbrechen						

Als Zertifikattyp wählen Sie "Zertifikatkette".

Abbildung 37

Assistent für ZA-Zertifikatinsta	Assistent für ZA-Zertifikatinstallation										
Schritte Hilfe	Schritt 4:Überprüfen der Einstellungen										
1. Token und Passwörter auswählen	Prüfen Sie hier Ihre Einstellungen. Klicken Sie auf 'Fertig stellen', um den Vorgang fortzusetzen.										
2. Eingabe der Zertifikatdaten	Konfiguration: TESTHOST										
3. Zertifikatstyp	Token: internal										
➡ 4. Überpr üfen der Einstellungen	Zertifikatstyp: Zertifikatkette										
5. Ergebnisse	Betreff: CN=TeleSec ServerPass CA 1,0U=Trust Center Services,0=T-Systems International GmbH,C=DE										
	Aussteller: CN=Baltimore CyberTrust Root,OU=CyberTrust,O=Baltimore,C=IE										
	Schlüsseltyp: RSA										
	Schlüsselgröße: 2048										
	Gültig ab: Tue Nov 30 17:24:37 CET 2010										
	Gültig bis: Thu Nov 30 17:23:46 CET 2017										
	Seriennummer: 07:27:42:C2										
	Fingerabdruck: E4:27:93:0D:7E:00:8F:D7:C9:64:69:5B:B7:AD:2F:93										
	Zurück Fertig stellen Abbrechen										

In Abbildung 37 werden alle Details des zu importierenden Zertifikats angegeben. Vergleichen Sie die Details mit den Einträgen auf unserer Internetseite:

<u>https://www.telesec.de/serverpass/</u> -> Support -> Root-/Sub-CA Zertifikate

Über "Fertig stellen" wird der Import abgeschlossen.





Der erfolgreiche Import wird entsprechend quittiert.

Das CA-Zertifikat wird nun entsprechend Abbildung 39 aufgelistet.

Abbildung 39

Konfigurationen > T	ESTHOST									
Virtuelle Server	Virtuelle Server HTTP-Listener Instanzen #		Allgemein	Leistung Zugriffssteuerung		ung Zertifikate	e J	Java Zusammenfa		
Serverzertifikate	Zertifikataussteller	CRL-Akt	tualisierungen	PKCS11-Token						
Die Seite listet die ve eine Zertifikatsperrlis werden, abgelaufene Zertifikatausste	TESTHOST - Zertifikataussteller (ZAs) Passwörter festlegen Die Seite listet die verschiedenen Zertifikataussteller auf, die in der Zertifikatdatenbank verfügbar sind. Sie haben auf dieser Seite die Möglichkeit, ein ZA-Zertifikat oder eine Zertifikate (Certificate Revocation List, CRL) zu installieren, oder Sie können ein ZA-Zertifikat löschen. Der Filter in der Tabelle kann dazu verwendet werden, abgelaufene Zertifikate anzuzeigen oder integrierte Zertifikate auszublenden.									
Installation	CRL wird installiert	Löschen	Filter: Inte	grierte Zertifikate	ausblenden 💌	[+@				
≶ ⊞ Pseudony	🗵 🗄 Pseudonym 🔺 Ablaufdatum 🛆 CRL 🗛									
TeleSec Se	erverPass CA 1 - Balti		30. November 2017 17:23:46 MEZ Nicht installiert							

Durch einen Klick auf das Zertifikat lassen sich die Zertifikatdetails anzeigen.

2.4 Installation des Serverzertifikats

Nun erfolgt der Import des Serverzertifikats

Öffnen Sie die Konfiguration des Virtuellen Servers und wählen den Reiter "Serverzertifikate", siehe Abbildung 40.

Konfigurationen > TESTHOST											
Virtuelle Server	rtuelle HTTP-Listener		Instanz	en	Allgemein	Leistung		Zugriffssteuerung		Zertifikate	Java
Serverzertifi	kate	Zertifikatau	issteller	CRL-Aktualisierungen PKCS11-Token							
TESTHOS	T - Ko	onfiguratio	on von S	Serv	erzertifikate	en				Passwörter f	estlegen
Zertifikate bes bescheinigen, besitzen, für C löschen.	tehen a dass d lients is	us digitalen E ler im Zertifika st das Zertifika)aten, die o at enthalten at optional.	den N ie öffe Auf d	lamen einer Per entliche Schlüss lieser Seite könr	son, ei el dies ten Sie	ner Firm er Entitä Serverz	na oder eine ät gehört. SS certifikate an	r anderen Er E-aktivierte \$ fordern, inst	ntität angeben ur Server müssen e allieren, erneuer	nd ein Zertifikat n und
Serverzei	rtifikat	te (0)									
Anforderung Installation Erneuern Löschen Filter: Alle Elemente											
Pseudonym Assteller Token Ablaufdat						Ablaufdatu	m				
Keine Zertifi Wählen Sie	kate ge die Ein	funden. Einig stellung "Alle	e Zeilen di Elemente"	eser in de	Tabelle sind mö er Filterliste, um	glicher alle Zei	weise ai Ien anzu	usgeblende uzeigen.	t, da ein Filte	er angewendet w	rurde.

In Abbildung 40 wählen Sie "**Installation**", ggf. ist die Angabe Ihres Passworts erforderlich.

Abbildung 41

Assistent für Serverzertifikatinstallation							
Schritte Hilfe	Schritt 1:Token und Passwörter auswählen						
 1. Token und Passwörter auswählen 	Die Seite zeigt die Liste mit den für die Konfiguration verfügbaren Token. Geben Sie das Passwort für das ausgewählte Token ein, sofern erforderlich.						
 Eingabe der Zertifikatdaten Zertifikatdetails 	Konfiguration: TESTHOST						
4. Überprüfen der Einstellungen	Token: internal 💌						
5. Ergebnisse	Vanien sie den Tokennamen aus der obigiert Liste. Wenn mit Schussen und in kaken, von Oracie Planet Web Server verwalteten Schlüsseldatenbank gespeichert ist, wählen Sie 'Intern'. Wenn Ihr Schlüssel auf einer Smartcard oder auf einem anderen externen Gerät gespeichert ist, wählen Sie den Namen des externen Tokens aus dem Dropdown- Listenfeld.						
	Passwort: Geben Sie das Passwort für das ausgewählte Token ein. Das Passwortfeld ist nur dann aktiviert, wenn das ausgewählte Token ein Passwort erfordert.						
	Zurück Weiter Abbrechen						

Hier wählen Sie den Token "internal", ggf. ist die Eingabe Ihres Passworts erforderlich.

. .

.

Schritte	Hilfe		Schritt 3:Eingabe der Zertifikatdaten	
 Konfigur Token ur auswähl 	ation ausv nd Passwö Ien	vählen örter	Geben Sie Zertifikatdaten im ASCII-Format zusammen mit den Headern im Te oder geben Sie den Pfad zu einer Datei an, welche die Zertifikatdaten enthält.	extbereich ein,
3. Eingabe	der Zertifi	ikatdaten	C Zertifikatdaten	
 Zertifikat Überprü Einstellu Ergebnis 	details fen der Ingen sse		BEGIN CERTIFICATE mdqZClkHJ0xmEIGFgQ9eXMBA45cJbjY04 y362AteQ/swTRpSRCyHz4DDkylJqt1/ly85/35nlZ9VLm /GMNJT9NdNRqDIA640EIGFgQ9eXMBA45cJbjY04 y362AteQ/swTRpSRCyHz4DDkylJqt1/ly85/35nlZ9VLm /GMNJT9NdNRqDIA640EIGFgQ9eXMBA45cJbjY04 y362AteQ/swTRpSRCyHz4DDkylJqt1/ly85/35nlZ9VLm /GMNJT9NdNRqDIA640 2+sUumyThhGT END CERTIFICATE	
			O Zertifikatsdatei	
			Pfad zur Zertifikatdatei auf dem Server	
			Zurück	Abbrecher

In das Feld "Zertifikatdaten" kopieren Sie das Zertifikat "**Ihr ServerPass Zertifikat**" incl. der ---BEGIN... und ---END... Zeilen (blau markiert) aus Abbildung 24.

Abbildung 43

Assistent für Serverzertifika	atinstallation
Schritte Hilfe	Schritt 3:Zertifikatdetails
1. Token und Passwörter auswählen	Wenn es sich um ein selbst signiertes Zertifikat handelt, geben Sie Pseudonym, Gültigkeit (in Monaten) und den HTTP-Listener zur Verarbeitung sicherer Anforderungen an.
2. Eingabe der Zertifikatdaten	* steht für Pflichtfelder
➔ 3. Zertifikatdetails	* Pseudonym: testhost-ssl
4. Überprüfen der Einstellungen	Listeners: http-listener-ss1 KEINER-
5. Ergebnisse	http-listener-1 http-listener-ssl
	Zurück Weiter Abbrechen

Für das zu importierende Serverzertifikat muss ein Pseudonym vergeben werden, z. B. testhost-ssl.

"

• •

Auch muss das Zertifikat an den HTTP-Listener gebunden werden, der für den SSL-Modus vorgesehen ist. Im Beispiel ist dies "http-listener-ssl".

Abbildung 44

Assistent	für Ser	verzertifikati	nstallation		
Schritte	Hilfe		Schritt 5:Überprüf	en der Einstellungen	
1. Konfiguration auswählen			Prüfen Sie hier Ihre Eins fortzusetzen.	stellungen. Klicken Sie auf 'Fertig stellen', um den Vorg	ang
2. Token ur auswähl	en en	orter			
3. Eingabe	der Zertifi	katdaten	Konfiguration: TE	STHOST	
			Pseudonym: tes	sthost-ssl	
4. Zertifikat	details		Token: inte	ernal	
➡ 5. Überprü	fen der		Listener: htt	p-listener-ssl	
Einstellu	ngen		Zortifikatdotaile		
6. Ergebnis	se		Retreff:	CN=testhost example com I =Musterstadt ST=BundesI	and OU=Muste
			Aussteller:	CN=TeleSec ServerPass CA 1,OU=Trust Center Servic	es,O=T-System
			Schlüsseltyp:	RSA	
			Schlüsselgröße:	2048	
			Gültig ab:	Wed Feb 20 16:25:17 CET 2013	
			Gültig bis:	Wed Feb 26 00:59:59 CET 2014	
			Seriennummer:	35:78:63:4F:87:8F:9C:33	
			Fingerabdruck:	EF:98:A3:54:52:BE:31:D7:A4:E2:5C:7D:72:2C:A8:C5	
			Servername:	[testhost.example.com]	
			•		Þ
			Zurück Fertig stel	llen	Abbrechen

In Abbildung 44 werden die Details Ihres Serverzertifikats dargestellt. Überprüfen Sie die Angaben und schließen den Import über "**Fertig stellen**" ab.

Abbildung 45



Der erfolgreiche Import wird entsprechend quittiert.

Konfigurationen > TESTHOST													
Virtuelle Server	e HTTP-Listener		Instanzen Allgemein		Le	Leistung		Zugriffssteuerung		Zerti	fikate	Java	
Serverzertif	ikate	Zertifikata	ussteller	CF	RL-Aktualisier	ingen	PKC	S11-1	Token				
TESTHOST - Konfiguration von Serverzertifikaten Passwörter festlegen Zertifikate bestehen aus digitalen Daten, die den Namen einer Person, einer Firma oder einer anderen Entität angeben und bescheinigen, dass der im Zertifikat enthaltene öffentliche Schlüssel dieser Entität gehört. SSL-aktivierte Server müssen ein Zertifikat besitzen, für Clients ist das Zertifikat optional. Auf dieser Seite können Sie Serverzertifikate anfordern, installieren, erneuern und löschen.													
Serverze	Serverzertifikate (1)												
Anforderun	g	Installation.	Erneu	iern	Löschen		ilter: All	le Ele	mente]		
≫ 🗄 Pse	udonyr	n 🔺	Aussteller			△ 1	oken		Ablauf	datum			
test	host-ss	il	TeleSec Se	erverP	ass CA 1	i	nternal		26. Fe	ebruar 201	4 00:59:5	9 MEZ	

So wie in Abbildung 46 gezeigt, wird das importierte Zertifikat nun unter "Serverzertifikate" aufgelistet.

Nun muss des SSL-Modus aktiviert werden. Wählen Sie hierfür den Reiter "**HTTP-Listener**", siehe Abbildung 47.

Abbildung 47

Konfigura	Konfigurationen > TESTHOST									
Virtuel Serve	le HTTP-List r	tener Instan	zen A	llgemein	Leistung	Zugriffss	teuerung	Zertifikate	Java	
TESTH Der Serve Server we eindeutig IP-Adress	TESTHOST - HTTP-Listener Der Server akzeptiert die HTTP-Anforderungen über einen HTTP-Listener, bevor die Anforderung an den konfigurierten virtuellen Server weitergeleitet wird. Auf dieser Seite können Sie HTTP-Listener hinzufügen und konfigurieren. HTTP-Listener müssen eine eindeutige Kombination aus Portnummer und IP-Adresse aufweisen. Sie können IPV4- oder IPV6-Adressen verwenden. Wenn Sie als IP-Adresse den Wert *** festlegen, wird ein HTTP-Listener erstellt, der alle IP-Adressen auf diesem Port überwacht.									
HTTP-	Listener (2)	_	_	_	_	_	_	_	_	
Neu	Löschen									
≶ 8	Name 🔺	IP-Adresse 🛆	Port 🛆	SSL 🛆	Standardmäß virtueller Ser	Siger ver 🛆	Servername	A Beschre	eibung 🛆	
	http-listener-1	* [Alle P. aressen]	80	Deaktiviert	TESTHOST		TESTHOST			
	http-listener-ssl	* [Alle IP-Adressen]	443	Deaktiviert	TESTHOST		testhost			

Falls wie in Abbildung 47 dargestellt, der SSL-Modus für den Listener "http-listener-ssl" auf "deaktiviert" steht, muss der SSL-Modus aktiviert werden. Wählen Sie den für SSL vorgesehenen HTTP-Listener aus, im Beispiel ist dies "http-listener-ssl".

Allgemein SSL							
HTTP-Listener bearbeiten - All	gemeine Einstellungen Ubernehmen Schließen						
Der Server akzeptiert die HTTP-Anforderungen über einen HTTP-Listener, bevor die Anforderung an den konfigurierten virtuellen Server weitergeleitet wird. Auf dieser Seite können Sie HTTP-Listener hinzufügen und konfigurieren. HTTP-Listener müssen eine eindeutige Kombination aus Portnummer und IP-Adresse aufweisen. Sie können IPV4- oder IPV6-Adressen verwenden. Wenn Sie als IP-Adresse den Wert *** festlegen, wird ein HTTP-Listener erstellt, der alle IP-Adressen auf diesem Port überwacht.							
	* steht für Pflichtfelder						
Allgemein							
Name:	http-listener-ssl 🔽 Aktiviert						
* Port:	443						
	Port, auf dem überwacht wird						
* IP-Adresse:	*						
	IP-Adresse oder * zur Überwachung auf allen IP-Adressen						
* Servername:	testhost						
	Name des Standardservers						
* Standardmäßiger virtueller Server:	TESTHOST V						
	Name des virtuellen Servers zur Verarbeitung von Anforderungen, für die kein Host gefunden wurde						
Beschreibung:							
	Geben Sie eine kurze Beschreibung für den HTTP-Listener ein.						

In der Konfiguration "HTTP-Listener bearbeiten" wählen Sie den Reiter "Allgemein" und aktivieren die Option "htt-listener-ssl". Als Port wird standartmäßig Port "443" verwendet. Alle anderen Angaben wählen Sie entsprechend Ihrer Konfiguration aus und übernehmen die Einstellungen.

Über den Reiter "**SSL**" lassen sich die Optionen für den SSL-Modus konfigurieren, siehe Abbildung 49.

Abbildung 49

Allgemein SSL	
HTTP-Listener bearbeiten - SSI Die Sicherheitseinstellung für den HTTP-Li × Allgemein × SSL2 × SSL3/TLS	L-Einstellungen Übernehmen Schließen stener kann nur aktiviert werden, wenn installierte Zertifikate verfügbar sind.
Allgemein	
Name:	http-listener-ssl
SSL:	✓ Aktiviert
Zertifikat:	RSA-Zertifikate: http-listener-ssl
Client-Authentifizierung:	ECC-Zertifikate: Es sind keine ECC-Zertifikate verfügbar O Erforderlich O Optional © Falsch
Authentifizierungs-Timeout:	60 Sekunden Das Timeout, nach dem der Clientauthentifizierungs-Handshake fehlschlägt [0.001-3600]
Maximum an Authentifizierungsdaten:	1048576 Die maximale Menge von Authentifizierungsdaten im Puffer. [0 - 2147483647]

Gemäß Abbildung 49 wird der SSL-Modus aktiviert und der zu verwendende http-Listener ausgewählt. Im Beispiel ist dies "http-listener-ssl".

Wählen Sie die übrigen Optionen gemäß Ihren Vorgaben aus und übernehmen die Änderungen über den entsprechenden Button.

.

VERSIC	ИС				STA	ARTSEITE	AKTUALISIERE	ABMELDE	N HILFE
Benutzer: admin Server: TESTHOST						Bereitstellung steht aus			
Oracl	Oracle iPlanet Web Server						en) werden aus	sgeführt 0	Ê
						Instanz(e	en) wurden ang	jehalten 塱 1	Java
	_	_	_	_	_	_	_	_	_
Konfigur	ationen > TESTH	OST							
Virtue	elle								
Serv	er HTTP-Lis	tener Instan	zen	Allgemein	Leistung	Zugriffs	steuerung	Zertifikate	Java
TEST	HOST - HTTP.	l istener							
Der Serv	ver akzeptiert die H	TTP-Anforderung	en über e	einen HTTP-Li	istener, bevor o	lie Anforder	ung an den kor	nfiaurierten virtı	uellen
Server w	eitergeleitet wird.	Auf dieser Seite kö	onnen Si	ie HTTP-Liste	ner hinzufügen	und konfigi	urieren. HTTP-l	Listener müss	en eine
IP-Adres	ge Kombination au se den Wert "*" fes	is Portnummer ur stlegen, wird ein H	ITTP-Lis	resse autweis stener erstellt,	der alle IP-Adr	i IPV4- oder essen auf d	iesem Port übe	n verwenden. v erwacht.	venn Sie als
		<u> </u>							
HTTP	-Listener (2)	_	_	_	_	_	_	_	
Neu.	Löschen								
					Standardm	äßiger			_
1	Name 🔺	IP-Adresse 🛆	Port .	ssl ⊿	virtueller Se	erver 🛆	Servername	e 🛆 Beschre	eibung 🛆
	http-listener-1	* [Alle	80		ESTHOST		TESTHOST		
		IP-Adressen]		Deaktivier	t				_
	http-listener-ssl	* [Alle IP-Adressen]	443	🛛 🛛 🖉 Aktivier	t ESTHOST		testhost		

Abbildung 50 zeigt den aktivierten SSL-Modus.

Abschließend muss die Konfiguration noch "bereitgestellt" werden. Dies geschieht über den entsprechenden Button oben rechts - "Bereitstellung steht aus".

Abbildung 51

Konfigurationsbereitstellung						
Bereitstelle	en einer Konfiguration für alle Instanzen					
	🔔 Bereitstellung steht aus					
	Die Konfiguration TESTHOST wurde lokal geändert. Klicken Sie auf "Bereitstellen", um die Änderungen für alle Instanzen zu übernehmen.					
	Bereitstellen Abb	rechen				

Über "Bereitstellen…" werden die Änderungen übernommen.

. . .



Ergebnisse	
i Die Konfiguration wurde erfolgreich auf all	en verfügbaren Knoten bereitgestellt.
	Schließen

Die Erfolgreiche Übernahme der Änderung wird entsprechend quittiert. Sie können das Fenster schließen.

Die Installation ist Abgeschlossen.

2.5 Sicherung der Dateien

Es wird dringend empfohlen, die erzeugten Dateien zu sichern, z. B. auf einem externen Medium!

Gesichert werden sollten die Schlüssel-Dateien des virtuellen Hosts, "cert8.db", "key3.db". und "secmod.db". In der Beispielkonfiguration befinden sie sich unter: C:\Program Files\Oracle\WebServer7\https-TESTHOST\config\

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 53-55) sowie im Internet Explorer (Abbildung 56-58) aufgeführt.

Firefox:

Abbildung 53 (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 54 (Firefox 18):



Wählen Sie "Zertifikat anzeigen".

Abbildung 55 (Firefox 18):

ertifikat-Ansicht:"testhost.example.com"	
Allgemein Details	
Zertifikatshierarchie	
Baltimore CyberTrust Root	Darstellung der
▲TeleSec ServerPass CA 1	kompletten
testhost.example.com	
	Zertifikatskette
Zertifikats-Lavout	
Atesthost example.com	
47ertifikat	
Version	
Seriennummer	
-Zertifikatsunterzeichnungs-Algorithmus	
4Validität	
-Nicht vor	
Nicht nach	Zertifikatdetails
Feld-Wert	
CN = TeleSec ServerPass CA 1	
OU = Trust Center Services	
0 = T-Systems International GmbH	
C = DE	
Exportieren	
Schließen	

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

<u>Abbildung 56</u> (IE 7, IE 8):	
COC V Ittps://testhost.example.com/	4

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

Über den Reiter "Details" lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 57.

. . .

Abbildung 57 (Die Zertifikatdetails)



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

Abbildung 58 (Die Zertifikatskette)

Zertifikat ? X Allgemein Details Zertifizierungspfad Zertifizierungspfad Baltimore CyberTrust Root E TeleSec ServerPass CA 1 E teleSec ServerPass CA 1 E testhost.example.com	Darstellung der kompletten Zertifikatskette
Zertifikat anzeigen Zertifizierungsstatus: Dieses Zertifikat ist gültig.	

So wie in Abbildung 58 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.

.