TeleSec ServerPass

Zertifikats-Erneuerung 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_erneu_inst_oracle_iplanet_7_we bserver.doc		Zertifikats-Erneuerung Oracle iPlanet 7 Webserver
Version	Stand	Status
1.1	14.04.2014	Final
Autor	Inhaltlich geprüft von	Freigegeben von
T-Systems International GmbH GCU Midmarket Public Health & Security, PSS - Trust Center Solutions	W. Bohn	L. Eickholt

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

Kurzinfo

Zertifikat Erneuerung 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	Allgem	eines	5				
	1.1 To	estzertifikate	6				
	1.2 S	pezielle Hinweise für Oracle iPlanet 7 Webserver	6				
2	Zertifik	at erneuern	7				
	2.1 B	edingungen für eine Zertifikatserneuerung	7				
	2.2 B	2.2 Besonderer Hinweis für eine Zertifikats-Erneuerung mit Oracle iPlanet 7					
	W	ebserver	7				
	2.3 E	rneuerung durchführen	8				
	2.3.0	Die Verwendung des Public Keys bei der Erneuerung	10				
	2.3.1	Erneuerung unter Wiederverwendung des Public Keys	10				
	2.3.2	Erneuerung unter Verwendung eines neuen Public Keys	10				
	2.4 In	nport des erneuerten Zertifikats	12				
	2.4.1	Herunterladen des erneuerten Zertifikats	12				
	2.4.2	Import des Serverzertifikats	14				
	2.5 Si	cherung der Dateien	18				
3	Kontro	le	19				

1 Allgemeines

Dieses Dokument beschreibt die Zertifikatserneuerung 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 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.

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

Die "ausstellenden Instanzen" (CA- und ggf. Root-Zertifikat) für TeleSec ServerPass wurden bereits korrekt installiert.

Sollten diese Zertifikate noch nicht installiert sein, so installieren Sie diese bitte vorab gemäß Anleitung "Oracle iPlanet 7 Webserver ->

Zertifikat-Requesterzeugung, Installation der Zertifikate".

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

2 Zertifikat erneuern

2.1 Bedingungen für eine Zertifikatserneuerung

Die Erneuerungsoption im Kundenportal kann <u>nicht</u> 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 eine 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 Zertifikat-Requests erforderlich. Folgen Sie hierzu bitte der Anleitung "Oracle iPlanet 7 Webserver -> Zertifikat-Requesterzeugung, Installation der Zertifikate".

2.2 Besonderer Hinweis für eine Zertifikats-Erneuerung mit Oracle iPlanet 7 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 "Oracle iPlanet 7 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 Servermanager 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. Die Zertifikatseinträge lassen sich durch Klicken auf die "Referenznummer" oder den "Common Name" anzeigen.

Abbildung 1 (Ausschnitt des Kundenportals):

Status:	alle	(exkl. abge	laufen) 💌			9	Suchen
Refnr. 🔻	Тур	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 3: (Zertifikatdetails)

Angaben zum Zer	tifikat
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 BASE	E64 kodierten Zertifikates inkl. der kompletten Zertifikatskette.
Download (nur Zei	rtifikat) Download (inkl. Zertifikatskette) Sperren Verlängern 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 4.

Abbildung 4:

Angaben zum Zert	tifikat				
Referenznummer	220002				
SubjectDN	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 z	zum Einlesen angeben):				
— ● Daten zum Ze	ertifikat				
ROOT-Auswahl *	TeleSec-CA-1				
Produktauswahl * CServerPass 3 Jahre Gültigkei 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 5.

. .

2.3.0 Die Verwendung des Public Keys bei der Erneuerung

Bei einer Erneuerung stehen zwei Optionen zur Auswahl, siehe Abbildung 5:

Abbildung 5: (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 eingeblendete 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.

Das Zertifikat wird i. d. R. sofort und ohne weitere Nachfrage ausgestellt und steht zum Download bereit. Hierzu klicken Sie auf die "ServerPass herunterladen".

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 bzw. ein neuer Request erzeugt werden.

Die Vorgehensweise wird erläutert in der Anleitung "Oracle iPlanet 7 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 1. 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. Wichtig sind die Angaben für "SubjectDN", siehe Abbildung 6. <u>Abbildung 6:</u> (Zertifikatsdetails)

Angaben zum Zert	tifikat	
Referenznummer	220002	
SubjectDN	bjectDN 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	

Nun muss ein neuer Request unter Berücksichtigung der hier ermittelten Daten erzeugt werden.

Die Erzeugung eines Serverschlüssels sowie eines Zertifikatrequests wird beschrieben in der Anleitung "Microsoft Internet Information Server (IIS) V7.0" \rightarrow "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: Request-Prüfung

Bitte überprüfen Si	e nach dem Einfügen des Requests die angezeigten Inhalte.
Mein PKC S#10 Zei	rtifikats-Request *
AjALBgIghkgBZQME, BZgKDIBRRd5RDtejt hXFXNtgF33ABSq4C nXQf9VWHfnbqbOsD mxkIJ7gsVQ17Ql/ml ZZDJigsOYJWpwWq0 wCKGkw/OB6YhUoQ sMp1uF/2 END NEW CERTIF	AQUwBwYFKw4DAgowCgYlKoZlhvdNAwowHQYDVR0OBBYEFGCn u8UVri1MA0GCSqGSlb3DQEBBQUAA4IBAQDRRifAlKxLmH8r cmTNWMhle+f1wHQ9D2TuJKi2v4LVET8WCtkF23E9XI9OO9gb /7AKnno9X9TmEzA7mkGe4khRH8vocPeTP+aDFuA5r8ojT95p EDo5xL6/vA2/DUKI2s28uQjVAglfdvzd8a0GrgyHzE+ztJ3 vpBXmP7I1RnJ+b3jNBfYf2xyiaI9umMDYbyMjoSTY7xve42D sQTW1fkwVBM1kUz4rqYiIA+oE2/510S1JvMYPIT0JU/cmn4IV FICATE REQUEST
Ihr Zertifikats-Req	uest wurde untersucht und enthält den nachfolgenden Inhalt
CN:	testhost.example.com
C:	DE
O :	Musterorganisation
OU1:	Musterorganisationseinheit
ST:	Bundesland
L:	Musterstadt
SAN 1(=CN):	testhost.example.com

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.

Nun werden alle weiteren Angaben (Produktauswahl, Laufzeit, Identifikationsangaben, Servicepasswort des zu verlängernden Zertifikats usw.) entsprechend Ihrer Vorgaben ausgewählt und der Auftrag abgeschickt.

Das Zertifikat wird i. d. R. sofort und ohne weitere Nachfrage ausgestellt und steht zum Download bereit. Hierzu klicken Sie auf die "ServerPass herunterladen".

2.4 Import des erneuerten Zertifikats

2.4.1 Herunterladen des erneuerten Zertifikats

Wie beschrieben, lässt sich das Zertifikat aus dem vorangegangen Dialog herunterladen bzw. erst nach Anmeldung im Portal "myServerPass":

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:	alle	(exkl. abge	laufen) 🔽				Suchen
Refnr. 🔻	тур	Neu/Ern.	CommonName	Techn. Kontakt	Ausgestellt	Ablauf	Status
220008	SSL	Ern.	testhost.example.com		01.02.2013	06.02.2014	akti∨

Wählen Sie das herunter zuladende Zertifikat durch Klick auf die Referenznummer aus.

Abbildung 9

Angaben zum Zer	tifikat
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	akti∨
Auftragstyp	Erneuerung des Auftrags mit RefNum 220002
Produkt	[ServerPass Standard, TeleSec-CA-1, 1 Jahr]
Techn. Kontakt	
Kaufm. Kontakt	
Download des BASI	E64 kodierten Zertifikates inkl. der kompletten Zertifikatskette.
Download (nur Ze	rtifikat) Download (inkl. Zertifikatskette) Sperren Verlängern Abbrechen

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

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

Wählen Sie das Format: "Download nur das Zertifikat". Aktivieren Sie die Option "Als Datei speichern und legen einen Dateipfad fest, z. B. c:\ Sie erhalten die Datei "servpass-123456.pem" und sie liegt nun unter c:\.

Die herunter geladene Datei enthält das Server-Zertifikat, wie in Abbildung 10 dargestellt.

Abbildung 10 (servpass-123456.pem)



2.4.2 Import des Serverzertifikats

Öffnen Sie die Konfiguration Console des Oracle iPlanet 7 Webservers,

siehe Abbildung 11.

In dieser Anleitung wird kein Passwort zum Schutz der Zertifikate vergeben. Wurde ein Passwort definiert, so muss es bei den nachfolgenden Aktionen immer wieder eingegeben werden.

Abbildung 11

Allgemeine Au	ıfgaben				
Klicken Sie auf die Sch	altfläche "i", um weiter	e Informatione	n zu einer Aufgabe zu ei	rhalten. Wenn Sie eine we	eitere Erläute
der remnitologie wund	chen, kicken ole mer.				
Konfigurationsaufga	aben		Virtuelle Serv	ver-Aufgaben	
Konfiguration auswäh	ilen: TESTHOST	• i	Virtuellen Ser	ver auswählen: TESTHO	ST 🔹 🚺
Konfiguration bearbei	ten	i	Virtuellen Ser	ver bearbeiten	ì
Neue Instanz		ì	Webanwend	ung hinzufügen	ì
Instanzen starten/anh	alten	i	Dokumentver	zeichnisse	ì
Java-Einstellungen be	arbeiten	i	CGI-Verzeich	nisse	i
Protokolleinstellungen	und Archivierung	i	URL-Umleitun	gen	i
Serverzertifikat anfor	dern	ì	Umgekehrter	Proxy einrichten	ì
Serverzertifikat instal	lieren	i	Zusammenfa	ssung anzeigen	ì
Zusammen fassung a	nzeigen	i			
Neue Konfiguration		1	Neuer virtuell	er Server	ì
6.0/6.1-Instanzen mig	rieren	i			
6.0/6.1-Instanzen mig	rieren	1			

Wählen Sie den Menüpunkt "Serverzertifikat installieren".

Es öffnet sich der Assistent für die Serverzertifikatinstallation, siehe Abbildung 12.

. .

Abbildung12

Assistent für Serverzertifikatinstallation					
Schritte Hilfe	Schritt 1:Konfiguration auswählen				
 1. Konfiguration auswählen 2. Token und Passwörter auswählen 	Wählen Sie eine Konfiguration in der Liste aus, für die Sie das Zertifikat installieren möchten. Der Konfigurationsname wird dem Text für die Zertifikatsignaturanforderung (Certificate Signing Request, CSR) hinzugefügt. Wenn keine Konfigurationen aufgelistet werden, schließen Sie diesen Assistenten, erstellen Sie eine Konfiguration, und führen Sie die Aktion erneut aus.				
3. Eingabe der Zertifikatdaten * steht für Pflichtfelder					
4. Zertifikatdetails	* Konfiguration auswählen				
5. Überprüfen der Einstellungen	TESTHOST				
6. Ergebnisse Wählen Sie eine Konfiguration aus der oben angezeigten Liste.					
	Zurück Weiter Abbrechen				

Wählen Sie Ihre Konfiguration aus.

Abbildung 13

Assistent für Serverzertifikatanforderung							
Schritte Hilfe	Schritt 1:Token und Passwörter auswählen						
 1. Token und Passwörter auswählen 	Die Seite zeigt die Liste mit den für die Könfiguration 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 lokalen, von Oracle Planet Web Server verwalteten Schlüsseldatenbank gespelichert ist, wählen Sie Intern: Wenn brischlüssel auf einer Smatracht oder auf einem anderen externen Gerät						
6. Ergebnisse	gespeichert ist, wählen Sie den Namen des externen Tokens aus dem Dropdown-Listenfeld.						
	Geben Sie das Passworf für das ausgewählte Token ein. Das Passwortfeld ist nur dann aktiviert, wenn das ausgewählte Token ein Passwort erfordert.						
	Zurück Weiter Abbrechen						

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

Abbildung 14

. . .

Oshsitta	Lilfo	Schritt 3:Eingabe der Zertifikatdaten
Schritte	HIITE	oonne olenigabe der Lertinkataden
1. Konfigur 2. Token ur auswähl	ation auswählen Id Passwörter en	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. Eingabe	der Zertifikatdaten	C Zertifikatdaten
4. Zertifikat 5. Überprüf 6. Ergebnis	details en der Einstellungen se	BEGIN CERTIFICATE MIIG9TCCBd2gAwlBAgIIPdM+izoPwP0wDQYJKoZIhvcNAQEFB QAwdjELMAkGA1UE BhMCREUxJTAj6gNVBAoTHFQtU3izdGVtcyBJbnRicm5hdGlvb mFsIEdfYkgxHjAc BgNVBAsTFVRydXN0IENIbnRiciBTZXJ2aWNIczEgMB4GA1UE AxMXVGVsZVNIYyBT2JC2NBLhMQLj2F+Y2J5uM4I2fZQHT fsPK599RObS0PShHa6OO+oTFJP9CV3Cqa14o0L/Jeo039kc 7gHbWzganu++mMDHP 06M4ZQE7umCX END CERTIFICATE
		C Zertifikatsdatei
		Zurück Waiter

. . .

In das Feld "Zertifikatdaten" kopieren Sie das Zertifikat "**Ihr ServerPass Zertifikat**" - incl. der ---BEGIN... und ---END... Zeilen - aus Abbildung 10.

Abbildung 25

Assistent für Serverzertifikatinstallation						
Schritte	Hilfe		Schritt 4:Zertifikatdetails			
1. Konfiguration auswählen		vählen	Wenn es sich um ein selbst signiertes Zertifikat handelt, geben Sie Pseudonym, Gültigkeit (in Monaten) und den HTTP-Listener zur Verarbeitung sicherer Anforderungen an.			
auswähl	en		1 Doppelte Serverdetails gefunden			
3. Eingabe	der Zertifi	katdaten	Es wurde ein Zertifikat mit denselben Serverdetails ermittelt. Es wird das vorhandene Zertifikatpseudonym verwendet, da nicht zwei Zertifikate mit identischen Serverdetails,			
➡ 4. Zertifika	tdetails		aber unterschiedlichen Pseudonymen vorliegen können.			
5. Überprü	fen der Eir	nstellungen	* stent fur Pflichtfelder			
6. Ergebnis	sse		* Pseudonym: testhost-ssi Listeners: http-listener-ssi KEINER http-listener-ssi http-listener-1			
			Zurück Weiter Abbrechen			

In Abbildung 25 merkt der Assistent an, dass bereits ein Zertifikat mit gleichlautenden Einträgen existiert wie im zu importierende Zertifikat. Das neue Zertifikat wird unter Verwendung des bestehenden Pseudonyms importiert.

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

Abbildung 26

Assistent für Serverzertifikatinstallation							
5	Schritte	Hilfe		Schritt 5:Überprüfen der Einstellungen			
1	. Konfigui	ration ausv	vählen	Prüfen Sie hier Ih	re Ei	nstellungen. Klicken Sie auf 'Fertig stellen', um den Vorgang fortzusetzen.	
2	. Token u auswäh	nd Passwi Ien	örter	Konfiguratio	n: T	ESTHOST	
3	. Eingabe	der Zertifi	katdaten	Pseudonym	te	esthost-ssl	
4	Zertifikat	details		Token:	ir	nternal	
	. Zoruma	laciano		Listener:	h	ttp-listener-ssl	
⇒ 5	. Überprü	fen der Ei	nstellungen	Zertifikatdet	ails		
6	Ergebni	sse		Betreff:		${\tt CN=} testhost.example.com, {\tt L=} {\tt Musterstadt}, {\tt ST=} {\tt Bundesland}, {\tt OU=} {\tt Musterorgani:} = {\tt Statestart}, {\tt ST=} {\tt Bundesland}, {\tt OU=} {\tt Musterorgani:} = {\tt Statestart}, {\tt ST=} {\tt Bundesland}, {\tt OU=} {\tt Musterorgani:} = {\tt Statestart}, {\tt ST=} {\tt Bundesland}, {\tt OU=} {\tt Musterorgani:} = {\tt Statestart}, {\tt ST=} {\tt Bundesland}, {\tt OU=} {\tt Musterorgani:} = {\tt Statestart}, {\tt ST=} {\tt Bundesland}, {\tt ST=} {\tt Statestart}, {\tt ST=} {\tt Statest$	
				Aussteller:		CN=TeleSec ServerPass CA 1,OU=Trust Center Services,O=T-Systems Intern :	
				Schlüsselty):	RSA	
				Schlüsselgr	öße:	2048	
				Gültig ab:		Thu Feb 21 12:34:02 CET 2013	
				Gültig bis:		Thu Feb 27 00:59:59 CET 2014	
				Seriennumn	ier:	3D:D3:3E:8B:3A:0F:C0:FD	
				Fingerabdru	ck:	7D:E5:BB:39:67:03:01:50:C7:F8:41:D2:96:84:4E:11	
				Servername	:	[testhost.example.com]	
				•))	
				Zurück Fer	tig st	ellen Abbrechen	

In Abbildung 26 werden die Details Ihres Serverzertifikats dargestellt. Überprüfen Sie die Angaben und schließen den Import über "**Fertig stellen**" ab.

Abbildung 27



Der erfolgreiche Import wird entsprechend quittiert.

Abschließend muss die Konfiguration noch "bereitgestellt" werden. Dies geschieht über den entsprechenden Button oben rechts - "**Bereitstellung steht aus**", siehe Abbildung 38.

Abbildung 38



Nachdem die Bereitstellung durchgeführt wurde stellt sich die "Konfiguration Console" wie folgt dar.

Abbildung 39

VERSION						STARTSE	ITE /	AKTUALISIER	EN ABMELDEN	HILFE
Benutzer: adm	Benutzer: admin Server: TESTHOST						Instanz(en) werden ausgeführt 1			
Oracle iP	lane	t Web Se	rver			Ins	stanz(en	ı) wurden ang	gehalten 壆 0	ju j
										Java
Konfiguration	en > TF	STHOST								
Troningaration										
Virtuelle Server	нтт	P-Listener	Instanze	en Allgemein	Leist	tung Zu	ugriffss	teuerung	Zertifikate	Java
Serverzertifi	ikate	Zertifikatau	ussteller	CRL-Aktualisierun	igen	PKCS11-1	Token			
TESTHOS	TESTHOST - Konfiguration von Serverzertifikaten Passwörter festlegen								stlegen	
Zertifikate bes	tehen a	us digitalen C	Daten, die d	len Namen einer Per	son, ein	er Firma od	ler einer	r anderen En	tität angeben un	
bescheinigen,	, dass d	ler im Zertifika	at enthalten	e öffentliche Schlüss	el diese	er Entität geh	nört. SSI	L-aktivierte S	erver müssen ei	n Zertifikat
löschen.	besitzen, für Clients ist das Zertifikat optional. Auf dieser Seite können Sie Serverzertifikate anfordern, installieren, erneuern und löschen.									
Serverzertifikate (1)										
Anforderung Installation Erneuern Löschen Filter: Alle Elemente										
≶ ⊞ Pse	eudonyr	n 🍐 /	Ausstallar				1			
2			Aussiener		Tol	ken 🛆	Ablaut	fdatum		

Der Import des erneuerten Zertifikats 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 40-42) sowie im Internet Explorer (Abbildung 43-45) aufgeführt.

Firefox:

Abbildung 40 (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 41 (Firefox 18):



Wählen Sie "Zertifikat anzeigen".

Abbildung 42 (Firefox 18):

Certifikat-Ansicht:"testhost.example.com"	
Allgemein Details	
Zertifikatshierarchie	
▲Baltimore CyberTrust Root	Darstellung der
⊿TeleSec ServerPass CA 1	kompletten
testhost.example.com	
	Zertifikatskette
Zertifikats-Layout	
▲testhost.example.com	
#Zertifikat	
Version	
Seriennummer	
Zertifikatsunterzeichnungs-Algorithmus	
Aussteller	
#Validität	
Nicht vor	Zortifikatdataila
Nicht nach	Zertinkatuetans
Feld-Wert	
CN = TeleSec ServerPass CA 1	
OU = Trust Center Services	
0 = T-Systems International GmbH	
C = DE	
Evportiaren	
Sghließen	

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 43</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 Abbildung44.

. . .

Abbildung 44 (Die Zertifikatdetails)



Über den Reiter "**Zertifizierungspfad**" lässt sich die Zertifikatskette prüfen, siehe Abbildung 54.

Abbildung 54 (Die Zertifikatskette)

Zertifikat	
Aligemein Details Zertifizierungspfad Image: ServerPass CA 1 Image: ServerPass CA 1 Image: ServerPass CA 1 Image: ServerPass CA 1	Darstellung der kompletten Zertifikatskette
Zertifikat <u>a</u> nzeigen	
Zertifizierungsstatus: Dieses Zertifikat ist gültig. OK	

So wie in Abbildung 54 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.

. . .