TeleSec ServerPass

Zertifikats-Requesterzeugung mit dem MS IIS 6.0



Version: 1.3 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_msiis_6.doc		Requesterzeugung Microsoft IIS 6.0 Webserver
Version	Stand	Status
1.3	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- systems.com
	* Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute	
Kurzinfo		

Kurzinfo

Zertifikats-Requesterzeugung mit dem MS IIS 6.0

T...

.

Änderungshistorie

. .

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	05.01.2011	W. Bohn	Erster Entwurf
1.0	20.01.2011	W. Bohn	Inhalt- und Layoutanpassung
1.1	27.01.2011	W.Bohn	Inhalt- und Layoutanpassung
1.2	12.02.2013	W. Bohn	Inhaltliche Anpassung
1.3	10.04.2014	M. Burkard	Anpassung der Links

Inhaltsverzeichnis

. .

. .

1	Allgemeines	5
	1.1 Testzertifikate	6
	1.2 Spezielle Hinweise für Microsoft IIS 6.0 Webserver.	7
2	Requesterzeugung, Beauftragung, Installation, Sicherun	g des privaten
	Schlüssels	8
	2.1 Requesterzeugung	9
	2.1.1 (*) Stichwort "Common Name"	13
	2.2 Beauftragung des Serverzertifikats	
	2.3 Herunterladen und Import des Server-Zertifikats	17
	2.3.1 Herunterladen des Server-Zertifikats	
	2.3.2 Import des Serverzertifikats	19
	2.4 Sicherung des Serverschlüssels incl. Serverzertifik	at22
3	Kontrolle	27

 \cdots T

1 Allgemeines

Dieses Dokument beschreibt die Requesterzeugung sowie die Einbindung der Zertifikate im Microsoft IIS 6.0 Webserver.

Der Ablauf im Microsoft IIS 5.0 verläuft ähnlich.

Bitte lesen Sie zuerst folgende Hinweise!

Sichern Sie Ihre Daten! Die Verwendung dieser Anleitung wurde hinreichend getestet. Jedoch kann für den unwahrscheinlichen Fall eines Datenverlustes keine Haftung übernommen werden.

Diese Anleitung beschreibt lediglich die Erzeugung eines Server-Zertifikat-Request sowie die Einbindung der Zertifikate im Webserver. Der Webserver ist somit in der Lage, verschlüsselte Verbindungen über https aufzunehmen. Weiterführende Erklärungen über den Einsatz von SSL-Zertifikaten zur Absicherung des Webservers entnehmen Sie bitte der Dokumentation des Webservers.

Bitte verwenden Sie für die Bearbeitung der Request- und Zertifikatsdateien einen möglichst einfachen Editor, zum Beispiel "vi" unter Linux/Unix bzw. "MS-Editor oder "Wordpad" unter Windows.

Wenn Sie Wordpad einsetzen, verwenden Sie stets die Option "Als Textdokument abspeichern".

Editoren aus Officepaketen können den Inhalt der Request- und Zertifikats-Dateien verfälschen und damit unbrauchbar machen.

Weiterhin beachten Sie bitte die in der CPS (**C**ertificate **P**ractice **S**tatement) gemachten Angaben bezl. des erlaubten Zeichensatzes ab Kapitel 8.3.

Weitere Informationen und Tipps erhalten Sie auf unserer Internetseite im "FAQ-Bereich".

Siehe hierzu: <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.

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 Microsoft IIS 6.0 Webserver

Die Beschreibung bezieht sich auf folgende Softwarekonstellation:

Microsoft Internet Information Server 6.0, deutsch Microsoft Server 2003 SP2, deutsch Internet-Explorer 7 oder höher

.

Voraussetzung: Der Webserver startet bereits im unverschlüsselten Modus.

Vor dem Import des Serverzertifikats ist ggf. der Import des CA-Zertifikats und evtl. auch des Root-Zertifikats erforderlich.

Die Einbindung von Root- und CA-Zertifikaten wird beschrieben in der Anleitung: "Microsoft Internet Information Server (IIS) V5.0 / V6.0" \rightarrow "Installation der CA-Zertifikate im IIS 5.0 u. IIS 6.0"

Siehe <u>https://www.telesec.de</u> \rightarrow ServerPass \rightarrow Support \rightarrow Downloadbereich

2 Requesterzeugung, Beauftragung, Installation, Sicherung des privaten Schlüssels

.

.

Während der Requesterzeugung werden die einzelnen Zertifikatsfelder abgefragt.

Alle hier eingetragenen Angaben erscheinen später unverändert im Zertifikat, im Einzelnen sind dies:

Beschreibung der Zertifikatseinträge:

"Gemeinsamer Name"	(*, 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 (Certificate Practice Statement) aufgeführten Hinweise. Insbesondere den erlaubten Zeichensatz. Siehe hierzu: <u>https://www.telesec.de/serverpass/support/downloadbereich/category/20-certification-practice-statement-cps</u>

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



2.1 Requesterzeugung

Zunächst öffnen Sie den Internetdienstemanager, siehe Abb.1. Diesen erreichen Sie über:

Start \rightarrow Verwaltung \rightarrow Internetdienstemanager

Abbildung 1:



Markieren Sie "Websites" und anschließend die abzusichernde Webseite.

Im Beispiel ist dies die "**Standardwebsite"**. Markieren Sie diese mit der rechten Maustaste und wählen dann "**Eigenschaften**". Es erscheint Abbildung 2.

Eigenschaften von Standardwebsite	? ×
Website Leistung ISAPI-Filter Basisverz Verzeichnissicherheit HTTP-Header Be	eichnis Dokumente enutzerdefinierte Fehler
Authentifizierung und Zugriffsteuerung Aktivierun Sie anonymen Zugang und bearbeiten Sie die Authentifizierungs- methoden für diese Ressource.	Bearbeiten
Einschränkungen für IP-Adressen und Domänennamen Gewähren oder verweigern Sie den Zugriff auf diese Ressource über IP-Adressen oder Internetdomänennamen.	Bearbeiten
Sichere Kommunikation Setzen Sie sichere Kommunikation voraus, und aktivieren Sie Clientzertifikate beim Zugriff auf diese Ressource.	Serverzertifikat Zertifikat anzeigen Bea <u>r</u> beiten
OK Abbrechen Ü	bernehmen Hilfe

Wählen Sie den Karteireiter "Verzeichnissicherheit" und dann unter "Sichere Kommunikation" den Button "Serverzertifikat...".

.

Daraufhin öffnet sich der IIS-Zertifikats-Assistent, siehe Abbildung 3.

Abbildung 3

Willkommen		×
	Willkommen	
	Dieser Assistent hilft Ihnen beim Erstellen und Verwalten von Serverzertifikaten, die in sicheren Webverbindungen zwischen Ihrem Server und einem Client verwendet werden.	
	Status des Webservers:	
	Auf dem Webserver ist kein Zertifikat installiert, und es stehen keine Anforderungen aus. Der Zertifikat-Assistent hilft Innen beim Erstellen eines neuen Zertifikats für den Webserver bzw. beim Anfügen an ein bereits vorhandenes Zertifikat.	
	Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.	
	< Zuriúck Weiter > Abbrecher	<u>,</u>

Es erfolgt eine kurze Erläutert der Funktionen des Zertifikat-Assistenten.

. .

414



In Abbildung 4 wählen Sie die Option "Neues Zertifikat erstellen".

Abbildung 5



In Abbildung 5 wählen Sie die Option: "Anforderung jetzt vorbereiten, aber später senden".

IIS-Zertifikat-Assistent	X
Name und Sicherheitseinstellungen Das neue Zertifikat muss einen Namen und eine Bitlänge haben.	
Geben Sie einen Namen für das neue Zertifikat ein. Der Name sollte einfach zu merken sein. Name:	
Standardwebsite Die Bitlänge des Schlüssels bestimmt die Verschlüsselungsstärke des Zertifikats. Je größer die Bitlänge ist desto größer ist die Sicherheit. Jedoch kann eine größere Bitlänge die Leistung weingern.	
Bitlänge: 1024 ▼ 512 1024 2048 ► Kryptografiedienst 4096 8192 16384	
< <u>Zurück</u> Weiter > Abbrech	en

In Abbildung 6 wird neben einem Zertifikatsnamen auch die Festlegung der Bitlänge (Schlüssellänge) des zu erzeugenden Schlüssels verlangt. Je nach verwendeter Version des IIS können mehrere Bitlängen ausgewählt werden.

Empfohlen wird eine Bitlänge von 2048, maximal jedoch 4096 Bit.

Requests mit einer Bitlänge kleiner 2048 Bit gelten nicht länger als sicher und sind von der Beauftragung ausgeschlossen

Das Häkchen für SGC (Server Gated Cryptography) wird nicht gesetzt.

In den nun folgenden Fenstern tragen Sie die Angaben entsprechend Ihrer Vorgaben ein und schließen die Requesterzeugung ab, siehe Abbildung 7 bis 12.

Abbildung 7

IS-Zertifikat-Assistent	
Informationen über Ihre Organisation	
Das Zertifikat muss Informationen über die Organisation beinhalten, die sie von anderen Organisationen unterscheidet.	S.
Geben Sie den Namen der Organisation und Organisationseinheit ein. Dies ist normalerweise der Name Ihrer Firma und der Name Ihrer Gruppe oder Abteilung	
Weitere Informationen erhalten Sie auf der Website der Zertifizierungsstelle.	
<u>O</u> rganisation:	
Musterorganisation	
O <u>rg</u> anisationseinheit:	
Musterorganisationseinheit	
	Abbrachan
	Abbrechen

.

Abbildung 8 (Festlegung des Common Name *)



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).

. .

IIS-Zertifikat-Assistent		×
Geographische Informationen Die Zertifizierungsstelle benötigt fol	gende geographische Informationen:	En:
Land/Region:		
DE (Deutschland)	•	
Bundesland/Kanton:		
Bundesland		
<u>O</u> rt:		
Musterstadt		
Bundesland/Kanton und Ort müsse dürfen keine Abkürzung enthalten.	en vollständige und offizielle Bezeichnungen sein und	
	< <u>Z</u> urück <u>Weiter</u> > Abbre	chen

Abbildung 10

IIS-Zertifikat-Assistent	×
Name der Zertifikatanforderungsdatei	
Die Zertifikatanforderung wird als eine Textdatei unter dem von Ihnen angegebenen Namen gespeichert.	
Geben Sie einen Dateinamen für die Zertifikatanforderung ein.	
Dateiname:	
c:\certreq.txt	D <u>u</u> rchsuchen
< <u>Z</u> urück	er > Abbrechen



Der Zertifikat-Assistent zeigten Einträge an, die später im Zertifikat erscheinen. Kontrollieren Sie diese und führen den Vorgang weiter.

Abbildung 12

IIS-Zertifikat-Assistent		×
	Abschließen des Assistenten für Webserverzertifikate	
	anforderung erstellt und in folgender Datei gespeichert: 🗾	
	c:\certreq.txt	
	Senden Sie diese Datei per Post oder E-Mail zu der Zertifizierungsstelle. Die Zertifizierungsstelle wird Ihnen dann eine Rückmeldungsdatei senden, die das neue Zertifikat enthält. Starten Sie diesen Assistenten erneut, um das Zertifikat zu Ihrem Server hinzuzufügen.	
	Klicken Sie auf "Fertig stellen", um den Vorgang abzuschließen.	
	< Zurück. [Fertig stellen] Abbrecht	m

Durch Klicken des Buttons "Fertig stellen" wird die Requesterzeugung abgeschlossen.

Öffnen Sie die Requestdatei z. B. mit dem Windows Editor, sie erreichen ihn über:

Start \rightarrow Alle Programme \rightarrow Zubehör \rightarrow Editor

. . .

Der Request stellt sich dar, wie in Abbildung 13 angegeben.

Abbildung 13 (certreq.txt)

—BEGIN NEW CERTIFICATE REQUEST— IUHILHJKGUTUGHJOILUOJHKLJLUOHJKHHLKKLHKKLHKLHKLU JHKHKKJLJKHKJHJKHJK786765HJKHKJHJKHJKHJKHJKHJKHJKJKK

KLMKLPZQW4onheuHZIIO5BugGDRDZ878GJHKFDRTSXY45dfdgfjj5677 —END NEW CERTIFIQATE REQUEST—

2.2 Beauftragung des Serverzertifikats

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

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

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.

Füllen Sie das Online-Formular entsprechend Ihrer Vorgaben aus.

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 13 inklusive der ----BEGIN.... und ----END... Zeilen per cut & paste.

Nach dem Einfügen werden die Request-Inhalte zur Kontrolle angezeigt, siehe Abbildung 14.

Bitte überprüfen Sie nach dem Einfügen des Requests die angezeigten Inhalte.		
Mein PKC S#10 Zert	ifikats-Request *	
AjALBgIghkgBZQMEA BZgKDIBRRd5RDtejtui hXFXNtgF33ABSq400 nXQf9VWIHnbqb05D7 mxkl/7gsvSQ17Q//mEI ZZDJigsOYJWpwWq0v wCKGkw/DD8YhUoQs0 sMp1uF/2 END NEW CERTIFI	QUwBwYFKw4DAgowCgYIKoZIhvoNAwowHQYDVR0OBBYEFGCn 8UVri1MA0GCSqGSIb3DQEBBQUAA4IBAQDRRifAIKxLmH8r mTNWMhle+f1wHQ9D2TuJkt2v4LVET8WCtkF23E9XI9OO9gb 7AKnno9X9TmE2A7mkGe4khRH8vocPeTP+aDFuA5r8ojT95p Do5xL6/4Z/DUKI2s28uQjVqJfdt/zd8a0GrgyHzE+ztJ3 pBXmP7I1RnJ+b3jNBIYf2xyiaI9umMDYbyMjoSTY7xve42D 2TW1fkwVBM1kUz4rqYiIA+cE2/510S1JvMYPIT0JU/cmn4IV CATE REQUEST	
CN:	testhost example com	
Ci.	DE	
0:	Musterorganisation	
001:	Musterorganisationseinheit	
ST:	Bundesland	
L:	Musterstadt	
SAN 1(=CN):	testhost.example.com	

Füllen Sie alle Kontaktfelder sowie alle Felder zur Auftragsprüfung entsprechen Ihrer 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.

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 mit den für den Download benötigten Angaben.

2.3 Herunterladen und Import des Server-Zertifikats

Achtung: Vor der Installation des Serverzertifikats ist der Import der ausstellenden Instanzen (CA-Zertifikat und ggf. auch das Root-Zertifikat) erforderlich. Hierzu ist eine separate Anleitung im Support Bereich verfügbar. www.telesec.de \rightarrow ServerPass \rightarrow Support \rightarrow Anleitungen Hier wählen Sie "Installation der CA-Zertifikate".

2.3.1 Herunterladen des Server-Zertifikats

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

Wählen Sie den Menüpunkt "Meine Zertifikate"

Hier werden nun alle Ihre Zertifikate aufgelistet. Wählen Sie das herunter zuladende Zertifikat durch Klick auf die Referenznummer aus, siehe Abbildung 15.

Abbildung 15:



Es werden zwei Download-Formate angeboten, siehe auch Abbildung 16:

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

Abbildung 16

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				

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 17 dargestellt.

Abbildung 17 (servpass-123456.pem)

-----BEGIN CERTIFICATE-----IUHILHJKGUTUGHJOILUOJHKLJLUOHJKHHLKKLHKKLHKLHKL U JHKHKKJLJKHKJHJKHJK786765HJKHKJHJKHJKHJKHJKHJKHJ KJK KLMKLPZQW4onheuHZIIO5BugGDRDZ878GJHKFDRTSXY45dfd gfjj5677 -----END CERTIFIQATE -----

2.3.2 Import des Serverzertifikats

Für die Installation des Serverzertifikats rufen Sie erneut die Eigenschaften der Standartwebseite auf. Dann den Reiter **Verzeichnissicherheit** und schließlich **Serverzertifikat**, siehe Abbildung 2.

Anschließend öffnet sich der IIS-Zertifikat-Assistent, siehe Abbildung 18.

Abbildung 18



Wählen Sie die Option: "Ausstehende Anforderung verarbeiten und Zertifikat installieren".



Wie in Abbildung 19 dargestellt, wählen Sie die Zertifikatsdatei aus, ggf. muss der Dateityp eingestellt werden auf "Alle Dateien (*.*)".

Abbildung 20

IIS-	Pertifikat-Assistent	X
Au	sstehende Anforderung verarbeiten	
	Ausstehende Zertifikatanforderung verarbeiten, indem die Datei ermittelt wird, die die Antwort der Zertifizierungsstelle enthält.	
	Geben Sie den Pfad und den Namen der Datei ein, die die Antwort der Zertifizierungsstelle enthält.	
	Pfad und Dateiname:	
	C:\serverpass-123456.pem	Durchsuchen
	< <u>Z</u> urück	r > Abbrechen

Folgen Sie dem Assistenten durch Klicken auf "Weiter", es erscheint Abbildung 21.

' '



In Abbildung 22 wird der zu verwendete Port für die SSL-Verbindung abgefragt. Standardmäßig wird der SSL-Port **443** verwendet.

Abbildung 22

IIS-Zertifikat-Assistent	×
Zertifikatzusammenfas Zertifikat soll von einer	sung Rückmeldungsdatei installiert werden.
Klicken Sie auf "Weite	r", um das folgende Zertifikat zu installieren.
Dateiname:	C:\servpass-123456.pem
Zertifikatdetails: Ausgestellt für Ausgestellt von Ablaufdatum Beabsichtigter Zweck Angezeigter Name Land/Region Bundesland/Kanton Stadt Organisation Organisationseinheit	testhost.example.com TeleSec ServerPass CA 1 18.02.2014 Clientauthentifizierung, Serverauthentifizierung Standardwebsite DE Bundesland Musterstadt Musterorganisation Musterorganisationseinheit
	< Zurück Weiter > Abbrechen

Abbildung 22 listet alle relevanten Daten des zu importierenden Zertifikats auf.

Folgen Sie dem Zertifikats-Assistenten bis zum Ende des Imports.

.



Nachdem der Webserver neu gestartet wurde, können verschlüsselte Verbindungen aufgebaut werden.

Es wird dringend empfohlen, den erzeugten Serverschlüssel zu sichern.

2.4 Sicherung des Serverschlüssels incl. Serverzertifikat

Nachfolgend wird die Sicherung aller Zertifikate incl. des privaten Schlüssels aufgezeigt.

Öffnen Sie den Internet Informationsdienste-Manager:

Start \rightarrow Verwaltung \rightarrow Internetdienstemanager

Markieren Sie die "**Standardwebseite"** mit der rechten Maustaste und wählen dann "**Eigenschaften**". Es erscheint Abbildung 21.

Abbildung 21



Hier wählen Sie den Reiter Verzeichnissicherheit und schließlich Zertifikat anzeigen, es erscheint Abbildung 22.



Achten Sie hier auf die korrekten Angaben für die Gültigkeit, "Ausgestellt für" und "Aufgestellt von".

Wichtig: Der Eintrag "Sie besitzen einen privaten Schlüssel für dieses Zertifikat" muss erscheinen!

Anschließend wechseln Sie auf den Reiter Details, es erscheint Abbildung 23.

Feld	Wert	<u> </u>
Version	V3	
Seriennummer	01 bc e8 60 d5 6a da ec	
Signaturalgorithmus	sha 1RSA	
Signaturhashalgorithmus	sha1	
Aussteller	TeleSec ServerPass CA 1, Tru	
Gültig ab	Friday, February 01, 2013 9:5	
Gültig bis	Friday, February 07, 2014 12:	
Antragsteller	testhost.example.com, Muster	<u> </u>

Wählen Sie die Option: "In Datei Kopieren" - es öffnet sich der Zertifikatexport-Assistent, siehe Abbildung 24.

.

Abbildung 24:

aten S	chlüssel exportieren	
õie kõn	nen den privaten Schlüssel mit dem Zertifikat exportieren.	
Private ausgev Seiten	: Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit vählten Zertifikat exportieren möchten, müssen Sie auf einer der folgen ein Kennwort eingeben.	: der den
Möchte	en Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?	
•	Ja, privaten Schlüssel exportieren	
C	Nein, privaten Schlüssel nicht exportieren	
	< Zurück Weiter >	Abl
		. 101

Wichtig: Im Dialogfenster Privaten Schlüssel exportieren wählen Sie:

"Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?"

"Ja, privaten Schlüssel exportieren"

Abbildung 25:

ormat	der zu exportierenden Datei
Zer	thikate konnen in verschiedenen Dateiformaten exportiert werden.
Wä	hlen Sie das gewünschte Format:
	C DER-codiert-binär X.509 (,CER)
	C Base-64-codiert X.509 (,CER)
	🔿 Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
	🔲 We <u>n</u> n möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
	Privater Informationsaustausch - PKCS #12 (.PFX) Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
	Privaten Schlüssel nach erfolgreichem Export löschen
	Alle erweiterten Eigenschaften exportieren
	C Microsoft Serieller Zertifikatspeicher (,55T)
eitere	Informationen über Zertifikatdateiformate
	< Zurück Weiter > Abbrechen

Im Dialogfenster "Format der exportierenden Datei" wählen Sie: "Privater Informationsaustausch – PKCS #12 (.pfx)" Und aktivieren lediglich die Option:

"Wenn möglich alle Zertifikate im Zertifizierungspfad einbeziehen."

Abbildung 26:

rtifikatsexport-Assistent	
Kennwort	
Der private Schlüssel muss mit einem Kennwort geschützt werden, um die Sicherheit zu gewährleisten.	
Geben Sie ein Kennwort ein und bestätigen Sie dieses.	
Kennwort:	

, Kennwort bestätigen:	

< Zurück Weiter > Abbr	echen

. . .

. .



Im Dialogfenster "Kennwort" wird ein Passwort für den exportierten Schlüssel festgelegt.

Achtung: Dieses Passwort wird bei einem ggf. erforderlichen Import benötigt!

Abbildung 27:

Zertifikatsexport-Assistent	×
Exportdatei Geben Sie die den Namen der zu exportierenden Datei an.	
Dateiname: c:\serverzertifikat.pfx	
< <u>Z</u> urück <u>W</u> eiter > Abbrec	hen

Abschließend wird noch ein Dateiname bzw. der Speicherort für die Sicherungsdatei vergeben, z. B. c:\serverzertifikat.pfx.

Abbildung 28

Zertifikatexport-Assistent	×
Der Exportvorgang wurde erfolgreich abgeschloss	en.
OK	

Wie in Abbildung 28 dargestellt, wird der erfolgreiche Export bestätigt.

Der Vorgang ist hiermit abgeschlossen.

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.

Exemplarisch ist hier die Darstellung im Firefox (Abbildung 29-31) sowie im Internet Explorer (Abbildung 32-34) aufgeführt.

Andere Browser stellen den SSL-Modus ggf. anders dar.

Firefox:

Abbildung 29 (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 30 (Firefox 18):



Wählen Sie "Zertifikat anzeigen".

Abbildung 31 (Firefox 18):

ifikat-Ansicht:"testhost.example.com"	×	
gemein Details		
Zertifikatshierarchie		
▲Baltimore CyberTrust Root		Darstellung der
⊿TeleSec ServerPass CA 1		kompletten Zertifi
testhost.example.com		kotokotto
		Kalskelle
Zertifikats-Layout		
▲testhost.example.com	<u> </u>	
#Zertifikat		
Version		
Seriennummer		
Zertifikatsunterzeichnungs-Algorithmus		
Aussteller		
#Validität		
·Nicht vor		Zertifiketeleteile
Nicht nach		Zertifikatoetalis
Feld-Wert		
CN = TeleSec ServerPass CA 1		
OU = Trust Center Services		
<pre>O = T-Systems International GmbH</pre>		
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 32</u> (IE 7, IE 8):	
COC V Ittps://testhost.example.com/	A

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

Über den Reiter "Details" lassen sich die Zertifikatsdetails anzeigen, siehe Abbildung 33.

. . .

Abbildung 33 (Die Zertifikatdetails)



Über den Reiter "**Zertifizierungspfad**" lässt sich die Zertifikatskette prüfen, siehe Abbildung 34.

Abbildung 34 (Die Zertifikatskette)

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

So wie in Abbildung 34 dargestellt, muss die gesamte Zertifikatskette präsentiert werden. Andere Browsertypen stellen die Zertifikatskette ggf. anders dar.

.



Wird die Zertifikatskette nicht korrekt angezeigt, so muss das CA-Zertifikat im Webserver importiert werden, siehe hierzu Anleitung:

"Microsoft Internet Information Server (IIS) V6.0" \rightarrow "Installation der CA-Zertifikate im IIS 6.0"

http://www.telesec.de/serverpass/support_downloads.html