SSL-geschützte Verbindungen mit dem "Internet Information Server" (IIS) unter Windows Server 2003

Dieses Dokument beschreibt, wie man mit dem IIS Zertifikatanträge (CSRs) erzeugt und aufgrund des CSR von der DFN-PKI generierte Zertifikate in den IIS einspielt.

Die hier gezeigten Bildschirmfotos sind mit einer englischen Version des Windows Server 2003 entstanden, die Vorgehensweise ist jedoch bei Windows Server 2008 und mit lokalisierten Versionen vergleichbar.

Administrator

Manage Your Server

💓 Windows Explorer

Command Prompt

Notepad

📝 WordPad

刻 My Computer

Gontrol Panel

administrative To

Printers and Faxes

() Help and Support

<u>∫</u> <u>S</u>earch

C Run...

1. Zertifikatsantrag erzeugen

Starten Sie die Management-Oberfläche des IIS:



Wählen Sie im Karteireiter "Directory

Security" die Aktion "Server Certificate":



Certification Authority
 Cluster Administrator
 Component Services
 Computer Management

Configure Your Server Wi

🔋 Internet Informati

Network Load Balancing Manager
 Performance
 Remote Desktops

Microsoft .NET Framework 1.1 Configural Microsoft .NET Framework 1.1 Wizards

Data Sources (ODBC)

bistributed File System

Local Security Policy Manage Your Server

80

Der "Web Server Certificate Wizard" wird gestartet. Fahren Sie mit "Next" fort:

"Create a

certificate" und bestätigen Sie mit

new

Wählen

"Next":

Sie



C Import a certificate from a Key Manager backup file.

C Import a certificate from a .pfx file

C Copy or Move a certificate from a remote server site to this site.

Wählen Sie "Prepare the request..." und bestätigen Sie mit "Next":



< Back

Next >

Cancel



Vergeben Sie einen (beliebigen) Namen, unter dem das Zertifikat im IIS bekannt gemacht werden soll. Setzen Sie die Schlüssellänge unbedingt auf 2048:

Hame and Security Settings Your new certificate must have a name and a specific bit length. Type a name for the new certificate. The name should be easy for you to refer to and remember. Name: Meine Website The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease perform Bit length: 2048 Select cryptographs serves provider (CSP) for this certificate	i Certificate Wia	ard			
Type a name for the new certificate. The name should be easy for you to refer to and remember. Name: Meine Website The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease perform. Bit length: 2048 C Select cryptograp as service provider (CSP) for this certificate	ame and Secu Your new certi	i ty Settings icate must have a name a	and a specific bit	length.	
Meine Website The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease perform Bit length: 2048 Select cryptographic service provider (CSP) for this certificate	Type a name f remember. Name:	or the new certificate. The	e name should be	e easy for you to n	efer to and
The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease perform use the stronger the security. However, a greater bit length may Bit length: 2048 Select cryptographic securic provider (CSP) for this certificate	Meine Websit				
Bit length: 2048 Select cryptographic service provider (CSP) for this certificate	The bit length The greater th decrease perfo	of the encryption key dete bit length, the stronger th rm	rmines the certifi he security. How	cate's encryption vever, a greater bi	strength. t length may
Select cryptographic service provider (CSP) for this certificate	Bit length:	2048	•		
	Select cryp	tograpriic service provide	r (CSP) for this c	ertificate	
			< <u>B</u> ack	Next >	Cancel

Geben Sie bei "Organization" "Universitaet Passau" exakt ein und bei "Organizational unit" den Namen Ihrer Einrichtung, z. B. "Lehrstuhl für Sicherheit":

Als "Common name" geben Sie den vollständigen Namen Ihres Servers ein, unter dem er im Internet bekannt ist:

Certificate Wizard	
)rganization Information	
Your certificate must include information a distinguishes it from other organizations.	about your organization that
Select or type your organization's name a legal name of your organization and the n	nd your organizational unit. This is typically the ame of your division or department.
For further information, consult certification	n authority's Web site.
Organization:	
Universitaet Passau	<u> </u>
Organizational unit:	
Einrichtungsname	-
	< Back Next > Cancel
Certificate Wizard	
Your Web site's common Name Your Web site's common name is its fully	qualified domain name.
Type the common name for your site. If the name. If the server is on the intranet, you name.	he server is on the Internet, use a valid DNS I may prefer to use the computer's NetBIDS
If the common name changes, you will n	eed to obtain a new certificate.
Common name:	
meinserver, einrichtung, uni-passau, de	
1	
	< Back Next > Cancel
Lostificato Winned	
Certificate Wizard	

Als "Geographical Information geben Sie bitte "DE (Germany)", "Bayern", "Passau" an, wie rechts dargestellt:

Certificate Wizard		
eographical Information The certification authority requires the	e following geographical information.	
Country/Region: DE (Germany)		
State/province:		•
City/jocality: Passau		•
State/province and City/locality must abbreviations.	be complete, official names and may not c	ontain
	< Back Next>	Cancel

Legen Sie hier den Namen fest, unter dem der CSR abgespeichert werden soll. Normalerweise können Sie den Systemvorschlag übernehmen:

the second	
Your certificate request is s specify.	ame aved as a text file with the file name you
Enter a file name for the ce	rtificate request.
Eile name:	
c: \certreq.txt	Browse
	< <u>B</u> ack <u>Next</u> Can
rtificate Wizard	
ertificate Wizard juest File Summary	
ertificate Wizard quest File Summary You have chosen to gener	ate a request file.
ertificate Wizard juest File Summary You have chosen to gener	ate a request file.
ertificate Wizard uest File Summary You have chosen to gener	ate a request file. equest. click Next.
ertificate Wizard Juest File Summary You have chosen to gener To generate the following r	ate a request file. equest, click Next.
ettificate Wizard juest File Summary You have chosen to gener To generate the following r File name: c:\certreq.bt	ate a request file. equest, click Next.
etificate Wizard uest File Summary You have chosen to gener To generate the following r File name: c:\cettreq.bt Your request contains the I	ate a request file. equest, click Next. following information:
ettificate Wizard uest File Summary You have chosen to gener To generate the following r File name: c:\certreq bit Your request contains the I Issued To Filerandt: Name	ate a request file. equest, click Next. following information: meinserver.einrichtung uni-passau.de
ettificate Wizard uest File Summary You have chosen to gener To generate the following r File name: c:\certreq.bt Your request contains the I Issued To Friendly Name Country/Region	ate a request file. equest, click Next. following information: meinserver.einrichtung.uni-passau.de Meine Website DE
ettificate Wizard uest File Summary You have chosen to gener To generate the following r File name: c:\certreq.bt Your request contains the I Issued To Friendly Name Country/Region State / Province	ate a request file. equest, click Next. following information: meinserver.einrichtung.uni-passau.de Meine Website DE Bayern.
rtificate Wizard uest File Summary You have chosen to gener To generate the following r File name: c:\certreq.bt Your request contains the I ssued To Fiendly Name Country/Region State / Province City Organization	ate a request file. equest, click Next. following information: meinserver.einrichtung.uni-passau.de Meine Website DE Bayern Passau Universitaet Passau
Intificate Wizard puest File Summary You have chosen to generate To generate the following r File name: c:\certreq bit Your request contains the I Issued To Friendly Name Country/Region State / Province City Organization Diraneicational Unit	ate a request file. equest, click Next. following information: meinserver.einrichtung.uni-passau.de Meine Website DE Bayern Passau Universitaet Passau Eriorichtungename
ettificate Wizard uest File Summary You have chosen to gener To generate the following r File name: c:\certreq bit Your request contains the I Issued To Friendly Name Country/Region State / Province City Organizational Unit	ate a request file. equest, click Next. following information: meinserver.einrichtung uni-passau.de Meine Website DE Bayern Passau Universitaet Passau Einrichtungsname
etificate Wizard uest File Summary You have chosen to gener To generate the following r File name: c:\cettreq.bt Your request contains the I Issued To Friendly Name Country/Region State / Province City Organization Organizational Unit	ate a request file. equest, click Next. following information: meinserver.einrichtung.uni-passau.de Meine Website DE Bayern Passau Universitaet Passau Einrichtungsname
etificate Wizard puest File Summary You have chosen to genera- To generate the following r File name: c:\certreq bit Your request contains the I Issued To Friendly Name Country/Region State / Province City Organizational Unit tificate Wizard	late a request file. request, click Next. following information: meinserver.einrichtung uni-passau.de Meine Website DE Bayern Passau Universitaet Passau Einrichtungsname < <u>Rack</u> <u>Next></u> Car

Prüfen Sie die Angaben und bestätigen Sie mit "Next":

Die Generierung des Zertifikatsantrags ist abgeschlossen, wenn nebenstehende Anzeige erscheint, die Sie mit "Finish" bestätigen:



2. Zertifikat beantragen

UNIVERSITÄT

M PASSAU

Mit dem Zertifikatantrag in der Datei certreq.txt können Sie nun über die Webschnittstelle der DFN-PKI ein Zertifikat beantragen, wie es im Dokument "Beantragung von Zertifikaten für Server der Universität Passau über den DFN-PKI-Dienst",* Abschnitt 3 bis 6, beschrieben ist.

- 4 -

^{*} siehe http://www.rz.uni-passau.de/fileadmin/Dateien/Dokumente/serverzertifikat_howto.pdf

3. Zertifikat im IIS installieren

Speichern Sie das von der DFN-PKI per E-Mail erhaltene Zertifikat (Mailanhang) zunächst lokal ab. Dann wählen Sie in der Management-Oberfläche des IIS bei den Eigenschaften Ihrer Website nochmals "Server Certificate":

"Web Server Certificate Wizard" Der informiert dass bereits Sie. ein Zertifikatsantrag vorliegt. Bestätigen Sie mit "Next":



 Web Site
 Performance
 ISAPI Filters
 Home Directory

 Documents
 Directory Security
 HTTP Headers
 Custom Errors

Enable anonymous access and edit the authentication methods for this resource.

Grant or deny access to this resource using IP addresses or Internet domain names.

Require secure communications an enable client certificates when this resource is accessed.

? ×

Edit.

Edįt...

ver Certificate.

E<u>d</u>it.

Default Web Site Properties

Authentication and access control

IP address and domain name restrictions

Documents

6

놂

Secure communications

Wählen Sie "Process the pending request...":

Geben Sie den vollständigen Dateinamen zu abgespeicherten Zertifikat dem ein (beachten Sie, dass der Dateiname mit .pem endet):



Geben Sie die Portnummer an, die für SSL-gesicherte Verbindungen genutzt werden soll (im Normalfall ist die Vorgabe 443 korrekt):



Bestätigen Sie die Richtigkeit der Zertifikatsdaten mit "Next":



Sie können die Zertifikatsinstallation mit "Finish" abschließen:



Sie sollten nun noch dafür sorgen, dass nur noch SSL-gesicherte Verbindungen zu Ihrem Server aufgebaut werden können. Wählen Sie dazu die Aktion "Edit":

ault web Sit	e propercies		
Web Site	Performance	ISAPI Filters	Home Directory
Documents	Directory Security	HTTP Headers	Custom Errors
Authenticati	ion and access control		
\$	Enable anonymous access ar authentication methods for t	nd edit the his resource.	Edit
IP address a	and domain name restrictions		
8	Grant or deny access to this IP addresses or Internet dor	resource using nain names.	
			Edit
Secure com	munications		
	Require secure communication enable client certificates whe	ns and <u>S</u> erv	er Certificate
	resource is accessed.	Уje	w Certificate
			Edb
		_	- Lucin

ad and

Markieren Sie "Require secure channel" und bestätigen Sie mit "OK":

Secure Communications	×
Require secure channel (SSL)	٦
Require 128-bit encryption	
Client certificates	
 Igngre client certificates 	
C Accept client certificates	
Require client certificates	
Client certricates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	
Current CTL:	
Neg Edj	
OK Cancel Help	

4. Zertifikatskette installieren

Damit das installierte Zertifikat von den Webbrowsern der Benutzer korrekt überprüft werden kann, müssen Sie noch einmalig die Zertifikate der sog. Zwischenzertifizierungsstellen installieren. Diese erhalten Sie, indem Sie mit dem Browser folgende Seite aufrufen:

https://pki.pca.dfn.de/uni-passau-ca/pub



Klicken Sie mit der rechten Maustaste auf "DFN PCA-Zertifikat" und speichern Sie mit "Save target as ..." die Datei "intermediatecacert.crt" auf der Festplatte ab.

Verfahren Sie ebenso bei "UNI-PASSAU CA Zertifikat": die betreffende Datei sollte als "cacert.crt" auf der Festplatte abgespeichert werden.

Öffnen Sie nun den Ordner, in dem Sie die beiden Dateien abgespeichert haben. Doppelklicken Sie auf die erste Datei "cacert.crt".

Es wird eine Information zu diesem Zertifikat Klicken Sie auf angezeigt. "Install Certificate ..."



Security Certificate Modified: Co. 45 20 60 60 60

Es startet der "Certificate Import Wizard". Klicken Sie auf "Next".







<u>File Edit View Favorites Tools</u>

Folders

Desktop
 My Documents
 My Computer
 My Network Places
 Recycle Bin

- 🗆 ×

💌 🔁 Go

Da

21 21

Size Type

2 KB Security Certificate 2 KB Security Certificate

Wählen Sie "Place all certificates in the following store" und klicken Sie auf "Browse...".

tificate	Import Wizard
Certific	ate Store
Cer	tificate stores are system areas where certificates are kept.
Wir	ndows can automatically select a certificate store, or you can specify a location for
	C Automatically select the certificate store based on the type of certificate
	Place all certificates in the following store
	Certificate store:
	Browse
	· · · · · · · · · · · · · · · · · · ·
	< <u>B</u> ack <u>N</u> ext > Cancel

Select Certificate Store

? X

Nun aktivieren Sie das Kästchen "Show physical stores" und wählen in der angezeigten Struktur "Local Computer" im Zweig "Intermediate Certification Authorities". Bestätigen Sie mit "OK".

Intermediate Certification Authorities
 Registry
 Group Policy
 Iocal Computer
 Trusted Publishers
 Untrusted Certificates
 Now physical stores
 OK Cancel

Select the certificate store you want to use.

Jetzt können Sie den vorhergehenden Dialog mit "Next" fortsetzen.

ificate I	mport Wizard	
Certificat	e Store	
Certif	icate stores are system areas where certificates are kept.	
Windo	ws can automatically select a certificate store, or you can specify a location for	
C	Automatically select the certificate store based on the type of certificate	
•	Place all certificates in the following store	
	Certificate store:	
	Intermediate Certification Authorities\Local Computer	
	_	
	< <u>B</u> ack <u>N</u> ext > Cano	el
		_

Sie können den "Certificate Import Wizard" jetzt mit "Finish" beenden.



Bestätigen Sie nun nochmals mit "OK".



Wiederholen Sie den Importiervorgang in der gleichen Weise mit der Datei "intermediatecacert.crt".

