Certificate Request Generation and Certificate Installation Instructions for IIS 5

April 14, 2006



1. Generating the Certificate Request

In this procedure, you will use the Internet Information Services (IIS) Console to generate a public and private key pair to support Secure Sockets Layer (SSL) encryption services. You will also generate the Public Key Cryptography Standard (PKCS) #10 certificate request and prepare it for submission to the Operational Research Consultants (ORC) External Certificate Authority (ECA).

1.1 Start the Internet Information Services Console

Click the **Start** button, point at **Programs**, and then point at **Administrative Tools**. From the submenu, click **Internet Services Manager**. The *Internet Information Services Microsoft Management Console* (MMC) displays.

1.2 Expand the Server

Services		
) 🗡 🖀 🗗 🗟	
Tree	Name	Path 🔺
Internet Information Services	 Scripts IISHelp IISAdmin IISSamples MSADC 	c:\inetpub\scripts c:\winnt\help\iishelp C:\WINNT\System32\inetsrv\iisadmin c:\inetpub\iissamples c:\program files\common files\system\msadc C:\Program Files\Common Files\Microsoft Shared\Web Se C:\WINNT\System32\RpcProxy C:\WINNT\web\printers

Figure 1-1. The Internet Information Microsoft Management Console

In the Console tree (the left panel), expand * *your server name*.

1.3 Open the Properties Dialog Box

Click the desired Web site. Right click the desired Web site and from the shortcut menu, click **Properties**. Alternately, click the **Action** menu and then click **Properties**. The **Administration Web Site Properties** dialog box appears.

Figure 1-2.	The Internet	Information	Management	Console

www.pki3.com Properties	s <u>? x</u>
Directory Security Web Site Operators	HTTP Headers Custom Errors Server Extensions Performance ISAPI Filters Home Directory Documents
Web Site Identification-	
Description:	www.pki3.com
IP Address:	137.242.16.166 Advanced
ICP Port:	80 SSL Port:
Connections	
C Limited To:	1,000 connections
Connection Timeout:	900 seconds
HTTP Keep-Alives	Enabled
Enable Logging —	
Active log format:	
W3C Extended Log	File Format
	OK Cancel Apply Help

Note: The SSL Port number may not be available at this time. If it is available to be set, then assign the SSL Port to **443**. This is the default port used for SSL communication.

1.4 Access the Directory Security Tab

Click the **Directory Security** tab. Under **Secure communications**, click **Server Certificate**.

Figure 1-3. The Directory Security Tab

www.pki3.com Properties	<u>?</u> ×
Web Site Operators Performance ISAPI Filters H Directory Security HTTP Headers Custom Erro	lome Directory Documents ors Server Extensions
Anonymous access and authentication control Enable anonymous access and edit the authentication methods for this resource.	[]
IP address and domain name restrictions Grant or deny access to this resource using IP addresses or internet domain names.	Edįt
Secure communications Require secure communications and enable client certificates when this resource is accessed.	<u>S</u> erver Certificate ⊻iew Certificate E <u>d</u> it
OK Cancel	Apply Help

1.5 The Welcome to the Web Server Certificate Screen

The **Welcome to the Web Server Certificate** wizard appears. Read the information and then click **Next**.

Figure 1-4. The Welcome to the Web Server Certificate Screen

Welcome to the Web Server	Certificate Wizard.	X
	Welcome to the Web Server Certificate Wizard	
	This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.	
	Status of your Web server:	
	Your Web Server doesn't have a certificate installed and you don't have any pending requests. Certificate Wizard will help you to create a new certificate for this Web Server or attach to an existing certificate.	
	To continue, click Next.	
	< Back Next > Cancel	

1.6 The IIS Certificate Wizard Screen

The **IIS Certificate** wizard appears. Confirm that the **Create a New Certificate** button is selected and then click **Next**.

Figure 1-5. The Create a New Certificate Screen

IIS Certificate Wizard	×
Server Certificate There are three methods for assigning a certificate to a Web site	
Select the method you want to use for this web site:	
< <u>B</u> ack	Next > Cancel

1.7 The Delayed or Immediate Request Screen

The **Delayed or Immediate Request** screen appears.

Figure 1-6. The Delayed or Immediate Request Screen

IIS Certificate Wizard				X
Delayed or Immediate You can prepare a req immediately.	Request uest to be sent later, or	you can send or	ne	
Do you want to prepar immediately to an onlin	e a certificate request to e certification authority?) be sent later, or '	r do you want to se	end it
Prepare the reques	st now, but send it later			
C <u>S</u> end the request i	nmediately to an online	certification auth	ority	
		< <u>B</u> ack	<u>N</u> ext >	Cancel

Click the **Prepare the request now, but send it later** button and then click **Next**. The **Name and Security Settings** screen appears.

1.8 The Name and Security Settings Screen

Figure 1-7. The Name and Security Settings Screen

IS Certificate Wizard	×
Name 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:	
www.yourwebserver.com	
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 performance.	
Bit length:	
Server Gated Cryptography (SGC) certificate (for export versions only)	
Charles Marks Course	. 1
<u> </u>	

Note: The default name given to this certificate is the name of the Web site that was selected, and the bit length is set to 512.

Click the **Bit Length** arrow and select **1024** for the bit length. Click **Next**. The **Organization Information** screen appears.

1.9 The Organization Information Screen

In the **Organization** box, type **U.S.** Government, and in the **Organizational Unit** box, type **<Your Company Name>**, **OU=ORC OU=ECA**.

Figure 1-8. The Organization Information Screen

IIS Certificate Wizard
Organization Information Your certificate must include information about your organization that distinguishes it from other organizations.
Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department. For further information, consult certification authority's Web site.
Organization:
U.S. Government
Organizational <u>u</u> nit:
USAF OU=PKI OU=DoD
< <u>B</u> ack <u>N</u> ext > Cancel

Click Next. The Your Site's Common Name screen appears.

Note: The text is case-sensitive. There is a space after the letters U.S. and the word Government. There is also a space after your company name and the letters OU=ORC. There is another space after the letters ORC and the letters OU=ECA.

1.10 The Your Site's Common Name Screen

In the **Common Name** text box, type the domain name of your Web site, for example, *www.testcompany.com* and then click **Next**. The **Common Name** is the Fully Qualified Domain Name (FQDN) of the server that the certificate will be installed on (e.g. *www.testcompany.com*).



IIS Certificate Wizard	×
Your 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 server is on the Internet, use a valid DP name. If the server is on the intranet, you may prefer to use the computer's NetBIO name. If the common name changes, you will need to obtain a new certificate. <u>Common name:</u>	4S S
www.basename.af.mil	
< <u>B</u> ack <u>N</u> ext >	Cancel

Click Next to display the Geographical Information screen.

1.11 The Geographic Information Screen



IIS Certificate Wizard		×
Geographical Information The certification authority requires the followin	g geographical information.	
<u>C</u> ountry/Region: US (United States) ▼		
<u>S</u> tate/province:		
		-
City/Jocality:		
		~
State/province and City/locality must be comp abbreviations.	olete, official names and ma	y not contain
	< <u>B</u> ack <u>N</u> ext :	> Cancel

Type the following information in the appropriate text boxes.

- In the Country/Region box, type US (United States). Normally, this does not need to be changed.
- In the State/province box, press Spacebar. To move to the City/locality field, press TAB or click the City/locality box.
- In the **City/locality** box, press **Spacebar**.
- Click Next. The Certificate Request File Name screen appears.

1.12 The Certificate Request File Name

In the **File name** box, enter a file name. Remember the folder where the file is saved. You may also click **Browse** to locate the desired folder. The file name should have a **.txt** extension and is saved in a text format. Click **Next**.



IIS Certificate Wizard		×
Certificate Request File Name Your certificate request is saved as a text file with the file name you specify.		
Enter a file name for the certificate request.		
<u>F</u> ile name:		
c:\certreq.txt	B <u>r</u> owse	
,		_
< Back	Next>	Cancel

1.13 The Request File Summary Screen

After a few moments, the **Request File Summary** screen appears. Read through the summary information on the screen.

- If changes need to be made, click **Back** as many screens as necessary to make changes.
- After making the changes, click **Next** as many times as needed to get back to this screen.
- Click **Next** to display the **Completing the Web Certificate Wizard** screen.

Figure 1-12.	The Request Fi	ile Summary Screen
--------------	----------------	--------------------

IIS Certificate Wizard		×
Request File Summary You have chosen to gene	rate a request file.	
To generate the following	request, click Next.	
File name:c:\certreq.txt		
Your request contains the	following information:	
Issued To Friendly Name Country / Region State / Province City Organization	www.afpki.kelly.af.mil www.pki3.com US U.S. Government	
Organizational Unit	USAF OU=PKI OU=D₀D	
	< <u>B</u> ack	lext > Cancel

1.14 The Completing the Web Server Certificate Wizard Screen

The screen informs you that the certificate request has been successfully completed. This screen displays the file folder and the file name of the certificate request. Click **Finish**.

Figure 1-13. The Completing the Web Server Certificate Wizard Screen



1.15 What's Next

At this point, you will use your Web browser to communicate with the *Certificate Authority* server to submit your certificate request. You will need to open **Windows Notepad** to copy and paste information from the clipboard during this operation.

2. Installing the Certificate in IIS5

In this section, you will install the certificate you retrieved (as per the notification email) to the *Microsoft IIS5* Web server. If you have not yet received your notification email do not attempt to perform these steps. You will need to start the **Internet Service Manager**.

Note: In this example, SSL is applied to the *Default Web Site*, which is the default Web site installed by *Windows NT/ IIS5*.

2.1 Start the Internet Information Service Manager

Click the **Start** button, point at **Programs**, and then point at **Administrative Tools**. From the submenu, click **Internet Services Manager**. The *Internet Information Services Microsoft Management Console* (MMC) displays.

2.2 Expand the Server

In the Console tree (the left panel), expand * your Web server name.

Figure 4-1. The Internet Information Microsoft Management Console

🚡 Microsoft Management Console -	[iis - Console Root\In	ternet Information Serve 💶 🗖 🗙
📸 <u>C</u> onsole <u>W</u> indow <u>H</u> elp		_ <u>_</u>
12 🖻 🖬 11 🕼		
🛛 🕶 Action 💌 View 🔤 🗶 😭 🖻		II 🛛 🍄 🔛 📑 🎿 🍖
Console Root	Name	Path 🔺
E Internet Information Server	🧕 default.asp	
⊡ <u>,</u> , ≝ ticweb	💽 postinfo.html	
E Default FTP Site	💽 _vti_inf.html	
	S IISSAMPLES	C:\Inetpub\iissamples
	IISADMIN	C:\WINNT\System32\inetsrv\iisadmin
	S IISHELP	C:\WINNT\Help
	G SCRIPTS	C:\Inetpub\scripts
	iisadmpwd	C:\WINNT\System32\inetsrv\iisadmp\
	🣴 msadc	C:\Program Files\Common Files\systen
🗄 🔂 Mail	🣴 Mail	C:\Inetpub\Mail
📄 🕀 🛅 cgi-bin	🚞 cgi-bin	
🕀 💼 images	🚞 images	
📄 💼 💼 Phone Book Servi 🖵	Den Phone Book Service	-
	<u>آ</u>	
Done		

2.3 Open the Properties Dialog Box

Right click the desired Web site and from the shortcut menu, click **Properties**. The selected **Web Site Properties** dialog box appears. Set the SSL Port to the number **443**.

Figure 4-2. The Website Properties Screen

Default Web S	ite Properties	? ×
Documents Web Site	Directory Security HTTP Head Operators Performance ISAPI F	ders Custom Errors Filters Home Directory
_ web Site Io Description IP Addres: ICP Port:	n: Default Web Site s: 192.168.0.16 80 SSL Port:	Advanced
Connection C Unlimit C Limited Connection	s ed I To: 1,000 connections n Timeout: 900 seconds	
Active lo	Logging og format: xtended Log File Format	Properties
	OK Cancel	Apply Help

Note: The SSL port is shown as 443, which is the default port for SSL function. This block may be grayed out if no certificate has ever been installed on this Web site. If so, you must return to this screen after the certificate is installed and set the SSL port to 443. Failure to do so will deny you access to your Web site when you turn SSL on.

2.4 Access the Directory Security Tab

Click the **Directory Security** tab

In the Secure communications section, click Server Certificate. This will display the Welcome to the Web Server Certificate Wizard.

Figure 4-3. The Directory Security Tab

www.pki3.com Properties	? ×
Web Site Operators Performance ISAPI Filters H Directory Security HTTP Headers Custom Err	Home Directory Documents ors Server Extensions
Anonymous access and authentication control Enable anonymous access and edit the authentication methods for this resource.	<u>Edit</u>
IP address and domain name restrictions Grant or deny access to this resource using IP addresses or internet domain names.	
	Edįt
Require secure communications and enable client certificates when this resource is accessed.	Server Certificate View Certificate E <u>d</u> it
OK Cancel	Apply Help

2.5 Initialize the Web Server Certificate Wizard

Click Next to display the Pending Certificate Request screen.





18

2.6 The Pending Certificate Request Screen

Select Process the pending request and install the certificate.

Click Next



IIS Certificate Wizard	×
Pending Certificate Request A pending certificate request is a request to wh authority has not yet responded.	ich the certification
A certificate request is pending. What would yo Process the pending request and install the Delete the pending request	ou like to do? e certificate
	< Back Next > Cancel

Click Next to display the Process a Pending Request screen.

2.7 The <u>Process a Pending Request</u> screen

Enter the file name and path of the certificate you saved in the previous section. Or, you may click **Browse** to find the certificate.

Figure 4-6. The Process a Pending Request Screen

IIS Certificate Wizard	×
Process a Pending Request Process a pending certificate request by retrieving the file that contains the certification authority's response.	
Enter the path and file name of the file containing the certification authority's respo	nse.
Path and file name:	
C:\sslcert.crt Bjows	ə
,	
(Pack	Cancel

Click Next to display the Certificate Summary screen.

2.8 The <u>Certificate Summary</u> Screen

Read the information contained in this screen and then click Next.

Figure 4-7. The Certificate Summary Screen

IIS Certificate Wizard	d	×
Certificate Summary You have chosen	y to install a certificate from a response file.	
To install the follow	ving certificate, click Next.	
File name:	C:\sslcert.crt	
Certificate details: Issued To Issued By Expiration Date Friendly Name Country / Region Organization Organizational Unit	win2ksrvr PKITIC Certificate Manager 10/2/2001 www.pki3.com US US US U.S. Governement USAF OU=PKI OU=DoD	
	< <u>B</u> ack <u>Next</u> >	Cancel

Note: If changes need to be made, click **Back** as many screens as needed and make the necessary changes. Click **Next** as many times as needed to return to this screen.

This will display the Completing the Web Server Certificate Wizard screen.

2.9 The Completing the Web Server Certificate Wizard Screen

Click Finish to return to the Directory Security tab.

Figure 4-8. The Completing the Web Server Certificate Wizard Screen



Notice that under the **Secure communications** section, the **View Certificate** and **Edit** buttons are now available.

2.10 The Edit Secure Communications Screen

Figure 4-9. The Directory Security Tab After Processing a Certificate Request

www.pki3.com Properties	<u>?</u> ×
Web Site Operators Performance ISAPI Filters H Directory Security HTTP Headers Custom Erro	fome Directory Documents ors Server Extensions
Anonymous access and authentication control	
Enable anonymous access and edit the authentication methods for this resource.	Edit
□ IP address and domain name restrictions	
Grant or deny access to this resource using IP addresses or internet domain names.	
	Edit
C Secure communications	
Require secure communications and enable client certificates when this	Server Certificate
resource is accessed.	View Certificate
	E <u>d</u> it
OK Cancel	Apply Help

In the **Secure communications** section, click the **Edit** button. The **Secure Communications** dialog box appears.

2.11 Enabling SSL Communications

- Click the **Require Secure Channel (SSL)** box.
- Click **Require 128-bit encryption**.

Note: Depending on your requirement you may need to require client certificates. Only select this option if you wish to restrict access to your web server to clients who have their own Identity Certificates.

• Click **OK** to return to the Web site properties screen.

Figure 4-10	The Secure	Communications	Screen
r_{1}		Communications	OCICEII

Secure Communic	ations
Require secure	channel (SSL)
Require <u>1</u> 28-b	it encryption
Client certificates -	
Ignore client of	ertificates
○ <u>A</u> ccept client	certificates
C Require client	certificates
Lient certificates accounts. This al using client certific Enable certific Current CTL:	ate trust list
Danon o L	,
	Ne <u>w</u> Edjt
	OK Cancel Help

Note: The DoD PKI and by extension the ECA PKI requires that 128-bit encryption algorithms be used.

2.12 Setting the SSL Properties

On the **Administration Web Site Properties** dialog box, click the **Web Site** tab. In the **SSL Port** field, make sure the number **443** is displayed. If not present, enter 443. This is the default port number for SSL communications.

Figure 4-11.	Assigning th	e SSL	Port Screen

www.pki3.com Propertie	es 🤶 🕺
Directory Security Web Site Operators	HTTP Headers Custom Errors Server Extensions Performance ISAPI Filters Home Directory Documents
Web Site Identification	
Description:	www.pki3.com
IP Address:	137.242.16.166
ICP Port:	80 SSL Port: 443
Connections	
<u> <u> U</u>nlimited </u>	
C Li <u>m</u> ited To:	1,000 connections
Connection Timeout:	900 seconds
HTTP Keep-Alive	s Enabled
Enable Logging -	
Acti <u>v</u> e log format:	
W3C Extended Lo	g File Format
[OK Cancel <u>A</u> pply Help

Click **OK**. Close the *Internet Information Manager* and save all settings.

At this point, the Web server is SSL enabled.

3. Obtaining and installing the ECA Root Certificate Chain

3.1 Trusted CA installation using the Windows Certificate Manager Import Wizard.

Note: Use this process only if procedure at section 5.1 does not work OR you simply prefer this method in lieu of section 5.1

Step 1. Download the Base 64 encoded certificate chain from the following URL: https://afpki.lackland.af.mil/assets/files/DoDcert_chainB64.zip

This file contains the DoD Class 3 Root and all the appropriate Intermediate CAs. It is updated as new CAs are added to the infrastructure.

Step 2. Use WinZIP to extract the Base 64 encoded certificate files.

The current list of CAs in the DoD PKI Trust Chain can be found at: <u>https://afpki.lackland.af.mil/html/rootchaininstallation.asp</u>

- Certificates identified as Root are installed as Trusted Root Certification Authorities in the Web server.
- Certificates identified with numbers such as CA-5, EMAIL CA-5, etc. are installed as Intermediate or Chaining CAs
- All certificates are placed in the Local Computer store to make them usable by all processes and users running on the computer.

Step 3. Start *Windows Explorer* and locate the Class3_Root_B64.cer file.

Note: This process must be performed as the Administrator.

Step 4. Double click on the .cer file to start the **Microsoft Certificate Wizard** process

Certificate ?X
General Details Certification Path
Certificate Information
This certificate is intended to:
 Ensures the identity of a remote computer Proves your identity to a remote computer Ensures software came from software publisher Protects software from alteration after publication Protects e-mail messages Allows data to be signed with the current time
Issued to: DoD CLASS 3 Root CA
Issued by: DoD CLASS 3 Root CA
Valid from 5/19/2000 to 5/14/2020
Install Certificate Issuer Statement
OK

Figure 5-1. The Certificate Information Screen

Click Install Certificate to display the Certificate Manager Import Wizard.

Step 5. The Certificate Import Wizard Screen

Figure 5-2. The Welcome to the Certificate Manager Import Wizard Screen



After reading the information on this screen, click **Next** to display the **Select the Certificate Store** screen.

Step 6. Select the Certificate Store Screen

Click **Place all certificates into the following store** and then click **Browse** to display the **Select a Certificate Store** screen.

Figure 5-3. The Select a Certificate Store Screen

Certificate Manager Import Wizard	×
Select a Certificate Store Certificate stores are system areas where ce	ertificates are stored.
Select the certificate store for the new certif	ïcates.
 Automatically select the certificate store 	ore based on the type of certificate
• Place all certificates into the following	g store
Certificate store:	<u>Browse</u>
	< <u>B</u> ack <u>N</u> ext > Cancel

- Select <u>Trusted Root Certification Authorities / local computer</u> for ROOT CA only.
- Select Intermediate Certificate Authorities / local computer for all other certificates such as CA-5, EMAIL CA-5, CA-6, EMAIL CA-6 etc.

Step 7. Select the Certificate Store Screen

Figure 5-4. The Select Certificate Store Screen

Select Certificate Store	? ×
Select a certificate store you wish to use	
Personal Trusted Root Certification Authorities Registry Cocal Computer Enterprise Trust Intermediate Certification Authorities Other People	•
Show Physical Slores	
OK Cano	cel

Click to place a checkmark in the **Show Physical Stores** box and expand the **Trusted Root Certification Authorities** list as shown and click **Local Computer**. Click **OK** to return to the **Select a Certificate Store** screen. The screen should look like the following:

Figure 5-5. The Select a Certificate Store after Selecting the Local Computer

Certificate Manager Import Wizard	×
Select a Certificate Store Certificate stores are system areas where certificates are stored.	
Select the certificate store for the new certificates.	
 Place all certificates into the following store Certificate store: 	
Trusted Root Certification Authorities\Local Computer Browse	
< <u>B</u> ack <u>N</u> ext > Cance	3

Click Next to display the Completing the Certificate Wizard Import screen.

Step 8. Completing the Certificate Wizard Import Screen

Click **Finish** to complete the import process.

Figure 5-6. The Completing the Certificate Manager Import Wizard Screen

Certificate Manager Import Wiz	ard		×
	Completing the Certific Import Wizard	cate Manager	
	You have successfully completed th Import wizard.	e Certificate Manager	
	You have selected the following for Certificate Store Selected by User Content	the import operation: Trusted Root Certificat Certificate	
	< <u>B</u> ack	-inish Cancel	

You will see the **Certificate Manager Import Wizard** confirmation screen reporting that the import process was successful. Click **OK**.

Figure 5-7. The Import Successful Screen

Certificat	e Manager Import Wizard	×
•	The import was successful.	
	[OK]	

Note: You must repeat this process (Steps 4 through 8) for the remaining Certificate Authority Certificates identified in Step 2

After all certificates have been installed, the server must be shut down and restarted.

This completes the installation process for the server.

4. Installing the DoD Root Certificate Chain in the Browser

All prospective users of your SSL-enabled Web site must accept the **DoD PKI Root Certificate Chain** in their browsers. These browsers must be U.S. High Encryption-capable (128-bit).

4.1 Using Internet Explorer

If you are using Microsoft Internet Explorer, you may install the root certificate chain by using the executable file found at

<u>https://afpki.lackland.af.mil/html/rootchaininstallation.asp</u>. This file may also be used for pushing the root certificate chain out across the entire domain using tools such as System Management Server (SMS).

4.2 Using Netscape Communicator

If you use a *Netscape* browser (4.06 or newer), follow the directions at <u>https://afpki.lackland.af.mil/html/import_netscape.asp</u>

Appendix A

Acronyms

CA	Certificate Authority
COMSEC	Communications Security
CRL	Certificate Revocation Lists
DoD	Department of Defense
FAQ	Frequently Asked Question
FQDN	Fully Qualified Domain Name
IA	Information Assurance
ID	Identification
IIS	Internet Information Services
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MMC	Microsoft Management Console
NIPRNet	Non-Classified Internet Protocol Router Network
OS	Operating System
OU	Organizational Unit
PKCS	Public Key Cryptography Standard
РКЕ	Public Key Enabling
PKI	Public Key Infrastructure
RA	Registration Authority
SIPRNet	Secret Internet Protocol Network
SMS	System Management Server
SPO	System Program Office
SSL	Secure Sockets Layer

TATrusted AgentURLUniform Resource LocatorUSAFUnited States Air Force