



Domino HTTP Hardware Cryptography Support using iSeries SSL

# **Copyright and Trademark Information**

# **Disclaimer; No Warranty**

THIS INFORMATION AND ALL OTHER DOCUMENTATION (IN PRINTED OR ELECTRONIC FORM) ARE PROVIDED FOR REFERENCE PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THIS INFORMATION, THIS INFORMATION AND ALL OTHER DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT ANY WARRANTY WHATSOEVER AND TO THE MAXIMUM EXTENT PERMITTED, IBM DISCLAIMS ALL WARRANTIES. INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SAME. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION, DIRECT, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES, ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS INFORMATION OR ANY OTHER DOCUMENTATION. NOTWITHSTANDING ANYTHING TO THE CONTRARY, NOTHING CONTAINED IN THIS INFORMATION OR ANY OTHER DOCUMENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF THE APPLICABLE LICENSE AGREEMENT GOVERNING THE USE OF THIS SOFTWARE.

Under the copyright laws, neither this documentation nor the software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part, without the prior written consent of IBM Corporation, except in the manner described in the documentation or the applicable licensing agreement governing the use of the software.

© Copyright IBM Corporation 1998, 2004

All rights reserved. Printed in the United States.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GS ADP Schedule Contract with IBM Corp.

#### Trademarks

The following items are trademarks of International Business Machines Corporation in the United States, other countries, or both:

iSeries	Lotus	Quickplace
iSeries Client Access	Lotus Notes	Notes
Power PC	Domino	
OS/400	Sametime Connect	

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

MMX is a trademark and Pentium is a registered trademark of Intel Corporation in the United States, other countries, or both.

Other product and company names mentioned herein may be the trademarks or registered trademarks of their respective owners.

# Domino HTTP Hardware Cryptography Support using iSeries SSL

This white paper provides an example of configuring Domino HTTP to use iSeries System SSL for the purpose of using a hardware cryptographic accelerator.

Domino is not aware of the cryptographic cards and does not need to be specially configured to use them. All it needs to do is be configured to use iSeries System SSL (referred to hereafter as System SSL). System SSL is in turn configured to use the cryptographic hardware. This configuration will function even if there is no configured cryptographic card in the system.

Important Note: Only Domino HTTP will use System SSL. All other Domino tasks will continue to use Domino's internal SSL function, and will not have access to the cryptographic hardware.

# **System Requirements**

- 5722-SS1 Option 34, Digital Certificate Manager
- 5722-DG1, IBM HTTP Server for iSeries
- 5722-AC2, Crypto Access Provider 56-bit for AS/400 or 5722-AC3, Crypto Access Provider 128-bit for AS/400
- Domino 6.5.2, 6.0.4, or later.
- A hardware cryptographic device. This includes the 4758 Cryptographic Coprocessor, or the 2058 Cryptographic Accelerator at the time of this writing.

# **Hardware Setup**

In order to use hardware cryptography (via System SSL) for the iSeries server, you must have the hardware cryptography cards correctly installed and configured. As of this writing, Domino for iSeries supports the 4758 Cryptographic Coprocessor and the 2058 Cryptographic Accelerator. The latest Cryptographic Hardware documentation can be found in the iSeries Information Center

(http://publib.boulder.ibm.com/html/as400/infocenter.html) under Networking->Networking Security. This example only covers the certificate creation for the 2058 Cryptographic Accelerator, or software-only encryption. Please refer to the documentation in the Information Center for installation and configuration of the 4758 Cryptographic Coprocessor.

### Step-by-step example scenario:

In this example we will:

- 1. Enable the DCM (Digital Certificate Management) server.
- 2. Create a local Certificate Authority (CA).
- **3.** Create a certificate store.
- **4.** Create a certificate for Domino using the 2058 Cryptographic Accelerator or software encryption.
- 5. Assign a certificate to Domino.
- 6. Configure Domino to use System SSL.
- 7. Configure the 2058 Cryptographic Accelerator.
- **8.** Follow links to information on configuring the 4758 Cryptographic Coprocessor.

# 1. Enable the Digital Certificate Management (DCM) server

DCM is configured using the \*ADMIN instance of the iSeries HTTP server. Start the \*ADMIN instance of the HTTP server if needed:

STRTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN)

The DCM server is accessed through your Web browser using port 2001. Internet Explorer is recommended. (Such as http://youriseries:2001. Figure 1)



Figure 1

# 2. Create a Local Certificate Authority (CA)

This section illustrates how to create your own Local certificate authority (CA) for issuing a certificate to use with Domino. Creating a local CA is a good way to test your SSL setup before purchasing a certificate from a trusted Internet CA.

From the HTTP Admin screen in the step above, click the "Digital Certificate Manager" link. (Figure 1)



#### Figure 2

Click "Create a Certificate Authority (CA)" from the left menu pane on Figure 2.

🚰 Digital Certificate Manager - Micros	oft Internet Explorer			
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>F</u>	<u>H</u> elp			
$\Leftrightarrow Back \ \bullet \ \Rightarrow \ \bullet \ \textcircled{O} \ \textcircled{O} \ \textcircled{O}$	↔ Back • → • 🙆 🛃 🖓 🚱 Search 🝙 Favorites 🦓 Media 🎲 🖏 • 🎒			
Address a http://lp18b1b:2001/QIBM/ICS	i5/Cert/Admin/qycucm1.ndm/main0 💽 🄗 Go Links »			
	Digital Certificate Manager @ IBM.			
	Select a Key Storage Location			
CALCULATION OF CONTRACTOR	Certificate type: Certificate Authority (CA)			
	Certificate store: Local Certificate Authority (CA)			
Select a Certificate Store	Select a method for storing the certificate's private key on the iSeries system.			
Expand All Collapse All	,			
▶ <u>Manage User Certificates</u>	C. C. C. C. L. Distribution for the form			
<ul> <li>Create New Certificate Store</li> </ul>	• Certificate store - Private key stored in software.			
<u>Create a Certificate Authority</u> (CA)	C Hardware - Private key stored in hardware.			
	C Hardware encrypted - Private key encrypted by			
▶ Manage CRL Locations	hardware master key and stored in software.			
<ul> <li>Manage PKIX Request Location</li> </ul>				
Return to iSeries Tasks	Continue Cancel			
Secure Connection				
🕙 Done	🛛 🖉 Local intranet 🥢			

Select "Certificate Store" on Figure 3 and click Continue. Note that if you do not have a 4758 Cryptographic Coprocessor in your system, that you may not see this screen. In that case, skip ahead to the next step.

🖉 Digital Certificate Manager	Microsoft Internet Expl	orer		
Eile Edit View Favorites Iools Help				
← Back • → • 🙆 😰 🖓	🔇 Search 📓 Favorites	💮 Media 🎯 🖏	• 🎒	
Address 🕘 http://lp18b1b:2001/	QIBM/ICSS/Cert/Admin/qycu	cm1.ndm/main0		🗾 🤗 Go 🛛 Links »
Digital Certificate Manager @ IEM. Create a Certificate Authority (CA)				0 IBM.
Active Contraction of the Contra	Certificate (	<b>ype:</b> Certificate Au	thority (CA)	
Select a Certificate Sto	e Certificate s	store: Local Certific	cate Authority (CA)	
Expand All Collapse A	The system w the Local Cer	rill create a certificat tificate Authority (C	e with a private key and s A) certificate store.	tore the certificate in
<ul> <li>▶ Manage User Certificates</li> <li>■ Create New Certificate Store</li> </ul>	Key size:	1024 💌 (bits)		
<u>Create a Certificate Authori</u> <u>(CA)</u>	store password:	*****	(required)	
<ul> <li>Manage CRL Locations</li> <li>Manage PKIX Request Locations</li> </ul>	ion Confirm	*****	(required)	
Return to iSeries Tasks		Certifi	icate Information	
Secure Connection	Certificate Authority (CA) name:	CA on LP18B1B		(required)
	Organizatio unit:	<b>n</b> iSeries Domino Te	am	
	Organizatio name:	n IBM		(required)
	Locality or city:	Rochester		
	State or province:	Minnesota		of 3 characters)
	region:	US (required)	)	
Validity period of Certificate Authority (CA) (2-7300): 1095 (days)				
Continue Cancel				
🙆 Done				🔂 Local intranet

Fill in the fields on Figure 4 with your system and business information. This certificate will be used as a root certificate for issuing other certificates (such as Domino's certificate). It is a good idea to distinguish in the name that it is a CA. Click Continue when done to bring up Figure 5.

🏄 Digital Certificate Manager - Micros	oft Internet Explorer		
<u>File Edit View Favorites Tools !</u>	Help (1997)		
⇔ Back → → → 🙆 😰 🖓 🛛 🎯 Sea	arch 🔝 Favorites 🛞 Media 🎯 🛃 🗸 🎒		
Address 🕘 http://lp18b1b:2001/QIBM/ICS	55/Cert/Admin/qycucm1.ndm/main0 🔽 🄗 Go Links »		
	Digital Certificate Manager 🛛 IBM.		
Carlower Car	Install Local CA Certificate		
	Certificate type: Certificate Authority (CA)		
Select a Certificate Store	Certificate store: Local Certificate Authority (CA)		
Expand All Collapse All	A certificate for your Certificate Authority (CA) was created and stored in the local Certificate Authority (CA) certificate store.		
Manage User Certificates  Create New Certificate Store  Create a Certificate Authority (CA)  Manage CRL Locations	You must install the Certificate Authority (CA) certificate in your browser so the browser can verify certificates that your CA issues. Click the following link to install the certificate in your browser. Your web browser will display several windows to help you complete the installation of the certificate.		
<ul> <li>Manage PKIX Request Location</li> </ul>	Install certificate		
Return to iSeries Tasks Secure Connection	After installing the certificate, select Continue so you can provide the policy data that will be used for signing and issuing certificates with this Certificate Authority (CA). Continue Cancel		
Done     Ccal intranet			



Since you have created your own CA, you need to tell your Web browser that your CA is trusted. Click "Install Certificate." If you are using Internet Explorer, you should see a box pop up (Figure 6):

File Down	load		x
?	Some files can h looks suspicious or save this file.	arm your computer. If the file information below s, or you do not fully trust the source, do not open	
	File name:	CA.cer	
	File type:	Security Certificate	
	From:	lp18b1b	
	1 This type of malicious of	f file could harm your computer if it contains ode.	
	Would you like to	o open the file or save it to your computer?	
	Open	Save Cancel <u>M</u> ore Info	
	✓ Al <u>w</u> ays ask	before opening this type of file	

Click Open.

Cert	ificate	<u>?</u> ×
Ge	eneral Details Certification Path	1
	Certificate Information	
	This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.	
	Issued to: CA on LP18B1B	-
	Issued by: CA on LP18B1B	
	Valid from 2/1/2004 to 2/1/2007	
	Install Certificate	nt
_		ĸ

Click "Install Certificate" on Figure 7. This will start a certificate import wizard (Figure 8). The following will guide you through the steps for Internet Explorer. Other browsers will vary.

# Certificate Import Wizard Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next. <a href="mailto:!>Beck\_Next">Lext</a> Cancel

#### Figure 8

Click Next.

Certificate Import Wizard	×
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for	
Place all certificates in the following store	
Certificate store:	
Browse	
< <u>B</u> ack <u>N</u> ext > Cancel	

Keep the default at "Automatically select the certificate store based on the type of certificate," and click Next.



Figure 10

Click Finish.



You will see a popup box about adding your certificate to the Root Store (Figure 11). Click Yes.



#### Figure 12

Another popup box will appear with the message "The import was successful." Click OK. You'll then be back at the screen where you started the certificate install. Click OK on Figure 12 to exit the installer.

On the DCM configuration screen that had the "Install Certificate" link, click Continue (Figure 5).

🖉 Digital Certificate Manager - Micros	oft Internet Explorer	_O×
<u>Eile Edit View Favorites Tools !</u>	Help	
↔ Back + → - 🙆 😰 🖓 🗐 🥸 Sea	arch 🔝 Favorites 🞯 Media 🎯 🔂 🗸 🎒	
Address Address http://lp18b1b:2001/QIBM/ICS	5/Cert/Admin/qycucm1.ndm/main0	▼ 🔗 Go Links »
	Digital Certificate Manager Certificate Authority (CA) Policy Data Your Certificate Authority (CA) was created with the	② IEM. default policy
Select a Certificate Store	data shown below. Change the data if you want and th Continue.	ien select
Expand All Collapse All Manage User Certificates Create New Certificate Store Create a Certificate Authority (CA)	Allow creation of user certificates:       C Yes         Validity period of certificates that are issued       365         by this Certificate Authority (CA) (1- (day: 2000):       (day: 2000);	• No 5)
Manage CRL Locations     Manage PKIX Request Location Return to iSeries Tasks  Secure Connection	Days until Certificate Authority (CA) expires: 1095	
Done	置 Loca	al intranet //,

Figure 13

Leave the values as the default on Figure 13. Click Continue.

🖉 Digital Certificate Manager - Micros	oft Internet Explorer
Eile Edit View Favorites Tools	Help
⇔ Back • → • 🙆 🛃 🥘 5e.	arch 👔 Favorites 🥘 Media 🧭 🛃 - 🎒
Address Address Address Address Address	55/Cert/Admin/qycucm1.ndm/main0 🗾 🔗 Go Links 🎽
	Digital Certificate Manager @ IEM.
	Policy Data Accepted
A State of the sta	Message The policy data for the Certificate Authority (CA) was accepted.
Select a Certificate Store	C.1 C
Expand All Collapse All	(*SYSTEM) and a server certificate signed by your Certificate Authority (CA). This will allow server authentication by users that use this system as a server.
▶ <u>Manage User Certificates</u>	
Create New Certificate Store	Continue Cancel
<u>Create a Certificate Authority</u> ( <u>CA</u> )	
▶ Manage CRL Locations	
Manage PKIX Request Location	
Return to iSeries Tasks	
Secure Connection	
E Done	🛛 🖉 Local intranet 🎢

You are done! Click Cancel, as we will not be continuing on from this screen.

# 3. Create a Certificate Store

On the left menu panel, click "Create New Certificate Store". (Figure 15)



Figure 15

Select \*SYSTEM and click Continue. If \*SYSTEM does not appear on this screen, then \*SYSTEM already exists. In that case, skip ahead to section 4, "Create a certificate for Domino using the 2058 Cryptographic Accelerator or software encryption."

🚰 Digital Certificate Manager - Micros	oft Internet Explorer
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>F</u>	telp 188
🗢 Back 🔹 🤿 🗸 🔯 🧟 Sea	rch 📾 Favorites 🛞 Media 🔇 🔂 🗸 🎒
Address Addres	5/Cert/Admin/qycucm1.ndm/main0
	Digital Certificate Manager 🛛 🛛 IBM.
	Create a Certificate in New Certificate Store
And Some	Certificate store: *SYSTEM
Select a Certificate Store	The new certificate store will contain the default list of Certificate Authority (CA) certificates. Do you want to create a certificate in
Expand All Collapse All	the certificate store?
a	• Yes - Create a certificate in the certificate store.
<u>Create Certificate</u>	• No - Do not create a certificate in the certificate store.
<u>Create New Certificate Store</u>	
<ul> <li><u>Install Local CA Certificate on</u> <u>Your PC</u></li> </ul>	Continue Cancel
▶ <u>Manage User Certificates</u>	
▶ <u>Manage CRL Locations</u>	
<ul> <li>Manage PKIX Request Location</li> </ul>	
Return to iSeries Tasks	
Secure Connection	
, One	Cocal intranet

Select "No - Do note create a certificate in the certificate store" on Figure 16, and click Continue.

🚰 Digital Certificate Manager - Micros	oft Internet Explorer	
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>F</u>	<u>H</u> elp	
🗘 Back 🔹 🔿 🖌 🙆 🚱 🖓 Sea	arch 📓 Favorites 🛞 Media 🧭	B- 3
Address 🙆 http://lp18b1b:2001/QIBM/ICS	iS/Cert/Admin/qycucm1.ndm/main0	▼ (∂Go Links »
	Digital Certific	cate Manager 🛛 🛛 IBM.
	Certificate Store Nam	e and Password
A SUTTER CONTRACTOR	Certificate store: *SYST	EM
Select a Certificate Store	You must enter a password the password again to confir	for the new certificate store and enter m it.
Expand All Collapse All	Certificate store	
■ Create Certificate	passworu.	(required)
<u>Create New Certificate Store</u>	Confirm password:	(required)
<ul> <li>Install Local CA Certificate on Your PC</li> </ul>		
▶ <u>Manage User Certificates</u>	<u>Continue</u> Cancel	
▶ <u>Manage CRL Locations</u>		
<ul> <li>Manage PKIX Request Location</li> </ul>		
<u>Return to iSeries Tasks</u>		
Secure Connection		
) e Done		🛛 🕅 🔠 Local intranet

Create a new password for the \*SYSTEM certificate store on Figure 17 and click Continue.

You will get a screen that says the certificate store has been created. Click "OK" to proceed. You will be back at the screen titled "Create New Certificate Store." You are now done creating the \*SYSTEM Certificate Store. Click "Cancel".

# 4. Create a certificate for Domino using the 2058 Cryptographic Accelerator or software encryption

This section explains how to create a certificate that is used by DCM and Domino. This certificate can be used with either the 2058 Cryptographic Accelerator, or with no cryptographic accelerator. This can be useful for testing on a system without an accelerator. The 2058 Cryptographic Accelerator is transparent to this certificate and will be used if configured and varied on.

Click "Select a Certificate Store" on the left menu panel.

🚰 Digital Certificate Manager - Microso	oft Internet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u>	lelp	10 A
⇐ Back	rch 🔝 Favorites 🎯 Media 🎯 🗟 🗸 🎒	
Address Addres	S/Cert/Admin/qycucm1.ndm/main0	▼ 🔗 Go Links »
	Digital Certificate Manager	0 IEM.
	Select a Certificate Store	
A Demo	Select the certificate store that you want to open.	
	O Local Certificate Authority (CA)	
Select a Certificate Store	⊙ *SYSTEM	
Expand All Collapse All	© Other System Certificate Store	
Create Certificate		
<u>Create New Certificate Store</u>		
Install Local CA Certificate on Your PC		
▶ <u>Manage User Certificates</u>		
▶ Manage CRL Locations		
<ul> <li>Manage PKIX Request Location</li> </ul>		
Return to iSeries Tasks		
Secure Connection		
J Cone		.ocal intranet

#### Figure 18

Select "\*SYSTEM" for the certificate store on Figure 18 and click Continue.

🚰 Digital Certificate Manager - Microso	oft Internet Explorer
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u>	lelp 🏭
← Back 🔹 → 🚽 🙆 🛃 📿 Sea	rch 📓 Favorites 🛞 Media 🎲 🖏 - 🎒
Address 🕘 http://lp18b1b:2001/QIBM/ICS	S/Cert/Admin/qycucm1.ndm/main0 🔽 🔗 Go Links »
	Digital Certificate Manager 🛛 🛛 IEM.
	Certificate Store and Password
Care Contraction of the Contract	Enter the certificate store password.
Select a Certificate Store	Certificate Server or client type:
Expand All Collapse All	Certificate <sub>*SYSTEM</sub> store:
	Certificate
Create Certificate	store path /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
<u>Create New Certificate Store</u>	filename:
<ul> <li>Install Local CA Certificate on Your PC</li> </ul>	Certificate
Manage User Certificates	store
Manage CPL Logations	password:
Manage DKIY Dequest Logation	Continue Reset Password Cancel
- Intanage FRIX Request Location	
Return to Denes 1 asks	
Secure Connection	
é	📄 📄 📴 Local intranet

Figure 19

Enter the password for the \*SYSTEM certificate store on Figure 19 and click Continue. You now have access to the certificate store.

🗿 Digital Certificate Manager - Micros	oft Internet Explorer
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools !	
🗢 Back 🔹 🔿 🚽 🙆 🖓 🧔 Sea	arch 🝙 Favorites 🛞 Media 🎲 🖏 - 🎒
Address 🚳 http://lp18b1b:2001/QIBM/ICS	55/Cert/Admin/qycucm1.ndm/main0 🔽 🔗 Go Links »
	Digital Certificate Manager <b>@</b> IBM.
	Current Certificate Store
ACT PROFESSION	You have selected to work with the certificate store listed below. The left
	frame is being refreshed to show the task list for this certificate store. Select
Select a Certificate Store	a task from the left frame to begin working with this certificate store.
	Certificate
Expand All Collapse All	type:
	Certificate *SYSTEM
▶ <u>Fast Path</u>	store:
<ul> <li><u>Create Certificate</u></li> </ul>	Certificate
<u>Create New Certificate Store</u>	and /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
<ul> <li>Install Local CA Certificate on Your PC</li> </ul>	filename:
▶ <u>Manage Certificates</u>	
Manage Applications	
Manage Certificate Store	
▶ Manage CRL Locations	
Manage PKIX Request Location	
Return to iSeries Tasks	
Secure Connection	
e	Local intranet

Click "Create Certificate" from the left menu panel on Figure 20.



Select "Server or client certificate" on Figure 21 and click Continue

🚰 Digital Certificate Manager - Micros	oft Internet Explorer					
<u>File Edit View Favorites T</u> ools I	Help					
🕁 Back 🔹 🔿 🚽 🙆 🕼 🔞 Sea	arch 🝙 Favorites 🛞 Media 🎲 🖏 - 🎒					
Address 🕘 http://lp18b1b:2001/QIBM/ICS5/Cert/Admin/qycucm1.ndm/main0						
	Digital Certificate Manager 🛛 🛛 IBM.					
	Select a Certificate Authority (CA)					
A State of the sta	Certificate type: Server or client					
	Certificate store: *SYSTEM					
Select a Certificate Store	Select the type of Certificate Authority (CA) that will sign this certificate.					
Expand All Collapse All						
	<ul> <li>Local Certificate Authority (CA)</li> </ul>					
▶ Fast Path	C VeriSign or other Internet Certificate Authority (CA)					
<u>Create Certificate</u>						
<ul> <li>Create New Certificate Store</li> </ul>						
<ul> <li>Install Local CA Certificate on Your PC</li> </ul>	Continue Cancel					
Manage Certificates						
▶ <u>Manage Applications</u>						
▶ <u>Manage Certificate Store</u>						
▶ <u>Manage CRL Locations</u>						
<ul> <li>Manage PKIX Request Location</li> </ul>						
Return to iSeries Tasks						
Secure Connection						
Cone Done	📴 Local intranet ///					

Select "Local Certificate Authority (CA)" on Figure 22 and click Continue. Note that this is where you would select to use a certificate purchased from an Internet Certificate Authority.



**Note** If there is no 4758 Cryptographic Coprocessor in your system, you will not see this screen. Continue on to the next step.

Select "Certificate Store - Private Key stored in software" on Figure 23 and click Continue. Note that this is the point where, if you were creating a certificate to use with the 4758, you would select "Hardware" or "Hardware encrypted." The 2058 does not require this step, as the certificate doesn't need to be aware of the 2058 existing.

🖉 Digital Certificate	Manager - Microso	oft Internet Explo	rer			
<u>File E</u> dit <u>V</u> iew F <sub>i</sub>	<u>a</u> vorites <u>T</u> ools <u>H</u>	elp				
🕁 Back 🔹 🤿 👻 🙆	) 🗗 🖧 🧔 Sea	rch 📓 Favorites	🛞 Media 🎯 🖏 🖬	<b></b>		
Address 🙆 http://lp18	3b1b:2001/QIBM/ICS	S/Cert/Admin/qycuci	m1.ndm/main0		💌 🧬 Go 🛛 Links 🎽	
	Digital Certificate Manager Ø IBM. Create Certificate					
A Stand	Con Martin	Certificate ty	<b>ype:</b> Server or client			
		Certificate s	tore: *SYSTEM			
Select a Certif	icate Store	Use this form t	o create a certificate	in the certificate store lis	ted above.	
Expand All C	ollapse All	Key size:	1024 💌 (bits)			
▶ Fast Path		Certificate label:	Lp18b1b Certificate		(required)	
Create Certificate			Certificate Info	rmation		
Install Local CA Ca	ate store		Cultineate Into			
<ul> <li>Manage Certificate</li> </ul>	s	Common name:	lp18b1b		(required)	
Manage Applicatio	ons	Organization			_	
Manage Certificate	Store	unit:	Domino for iSeries			
Manage CRL Locat	tions	Organization	IBM		(required)	
<ul> <li>Manage PKIX Req</li> </ul>	uest Location	name: Locolity or				
Return to iSeries Tasl	ks	city:	Rochester			
		State or	Minnocoto		(required:minimum	
Secure Connect	tion	province:	Immesora		of 3 characters)	
		Country or region:	US (required)			
			Subject A	Alternative Name		
		<b>Note:</b> Certific but are recom	ate extensions are not mended for Virtual P	t necessary for Secure S rivate Network (VPN).	ockets Layer (SSL),	
		IP version 4	address:			
		Fully qualifie	ed domain name:			
		(host_name.d	omain_name)			
		E-mail addre (user_name@	ss: domain_name)			
		Continue	Cancel			
۲					🕃 Local intranet 🥢	



Fill in the screen on Figure 24 with information about your system and company. You can pick a key size of your choice. The "Subject Alternative Name" can be left blank for this example. Click Continue.

🚰 Digital Certificate Manager - Microsofi	t Inte	rnet Explorer				
File Edit View Favorites Tools Help						
😓 Back 🔹 🔿 🖉 🖉 🖓 🔯 Search 👔 Favorites 🛞 Media 🎲 🖏 🚽						
Address 🕘 http://lp18b1b:2001/QIBM/ICS5/	Cert/A	dmin/qycucm1.ndm/main0		▼ 🖓 Go Links »		
	Digital Certificate Manager @ IBM.					
		Directory Services server	Server	None assigned 🗖		
And the second s		Directory Services publishing	Client	None assigned		
		Directory Services client	Client	None assigned		
Select a Certificate Store		OS/400 VPN Key Manager	Server	None assigned		
Expand All Collapse All		Enterprise Identity Mapping (EIM)	Client	None assigned		
		OS/400 TCP/IP FTP Server	Server	None assigned		
▶ <u>Fast Path</u>		OS/400 TCP/IP FTP Client	Client	None assigned		
<u>Create Certificate</u>		Webserver Search Engine	Server	None assigned		
Create New Certificate Store		HTTP Server Monitor	Server	None assigned		
Your PC		QIBM_HTTP_SERVER_ADMIN	Server	None assigned		
▶ <u>Manage Certificates</u>				]		
Manage Applications Continue Cancel						
Manage Certificate Store						
e				E Local intranet		

This next screen (Figure 25) is titled "Select Applications." We will do this after we create an application identifier for Domino. For now, do not check any boxes. Click Continue.

🚰 Digital Certificate Manager - Microso	ft Internet Explorer	_ 🗆 🗵
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> e	lp	
⇐ Back	th 🔝 Favorites 🎯 Media 🎯 🖏 🚽 🎒	
Address a http://lp18b1b:2001/QIBM/ICSS	/Cert/Admin/qycucm1.ndm/main0	▼ 🔗 Go Links »
	Digital Certificate Manager	0 IEM.
	Application Status	
	Message The applications you selected will use this	certificate.
Select a Certificate Store	ОК	
Expand All Collapse All		
▶ <u>Fast Path</u>		
Create Certificate		
é	Loc	al intranet //.

Click OK on Figure 26. You are now done and have a certificate that will work with software encryption or with the 2058 Cryptographic Accelerator. You will be back at the "Create Certificate" screen. Click Cancel to exit.

# 5. Assign a certificate to Domino

The iSeries DCM uses Applications Identifiers (AppID) to associate a certificate with an application. We will now create a new AppID for Domino.

Click "Manage Applications" from the left menu panel on figure 27.



Figure 27

Select "Add application" on Figure 27 and click Continue.

🚰 Digital Certificate Manager - Microsol	ft Internet Explorer
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> e	lp 👔
↔ Back • → - 🔕 😰 🖓 🔞 Searc	:h 📷 Favorites 🛞 Media 🔇 🔂 - 🎒
Address 🙆 http://lp18b1b:2001/QIBM/ICS5	/Cert/Admin/qycucm1.ndm/main0 💌 🔗Go Links »
	Digital Certificate       IEM.         Add Application       Select the type of application that you want to add.
Select a Certificate Store	<ul> <li>Server - Add a server application</li> <li>Client - Add a client application</li> </ul>
Expand All Collapse All	Continue
Fast Path     Done	Local intranet

Select "Server" on Figure 28 and click Continue.

🗿 Digital Certificate Manager - Microsoft Internet Explorer					
<u>File Edit View Favorites Tool</u>	s <u>H</u> elp	10 A			
🕁 Back 🔹 🤿 🖌 🙆 🕼 🔇	)Search 📷 Favorites 🍘 Media 🧭 🗟 🛛 🎒				
Address 🕘 http://lp18b1b:2001/QIBM	1/ICSS/Cert/Admin/qycucm1.ndm/main0	▼ 🖓 Go Links »			
Digital Certificate Manager Ø IBM.         Add Application         Application type: Server         Application The DOMINO					
Select a Certificate Store					
Expand All Collapse All	Exit program information				
	Exit program: *NONE				
▶ <u>Fast Path</u>	Exit program library:				
Create Certificate     Create New Certificate Store	Threadsafe: No 💌				
Install Local CA Certificate on Your PC	Multithreaded job action:	•			
▶ <u>Manage Certificates</u>	<u>L_1L</u> /L				
<ul> <li>Manage Applications</li> <li>View application definition</li> </ul>	Application user profile: QNOTES				
<ul> <li>Update certificate assignment</li> </ul>	Define the CA trust list: O Yes © N	>			
<ul> <li>Define CA trust list</li> <li>Add application</li> </ul>	Client authentication supported: • Yes O No	>			
<ul> <li><u>Remove application</u></li> </ul>	Client authentication required: O Yes O N	0			
<ul> <li>Update application definition</li> <li>Validate application</li> </ul>	Certificate revocation processing: O Yes © N	2			
Manage Certificate Store					
▶ Manage CRL Locations	an application description.	mormation or			
<ul> <li>Manage PKIX Request Location</li> </ul>	Application description message information				
Return to Series Tasks	Message file:				
	C Message file library:				
	Message ID:				
	Application description:     Domino				
Add Cancel					
		arintranet //			



Fill in the fields on Figure 29 as shown above. You can choose to require client authentication if needed. Please note the Application ID specified at the top of the page (DOMINO in our example). You will need this name to configure Domino in a later step. Also note that the "Application User Profile" needs to be set to QNOTES.

This will give Domino access to the \*SYSTEM certificate store files. Click Add to continue.

You should receive a message that the application has been added. Click OK.

We are now back at the Manage Applications screen. We need to assign the certificate we created earlier to Domino's AppID that we just created. Select "Update certificate assignment" on Figure 30 and click Continue.



Figure 30

Select the type of application that you want to update on Figure 31. Select "Server" and click Continue.



Figure 31

On Figure 32, pick Domino as the Application and click "Update Certificate Assignment."

🚰 Digital Certificate Manager - Micros	oft Internet Explorer				
Eile Edit View Favorites Tools H		<b>*</b>			
⇔ Back ▼ ⇒ ▼ ③ ☑ △ ○ Q Sea	rch 📷 Favorites 🎯 Media 🎲 🗈 🗃	- Co Links »			
Address Thttp://fp18b1b:2001/QIBM/ICS5/Cert/Admin/qycucm1.ndm/main0 Provide Unks " Digital Certificate Manager Provide Unks " Application type: Server Select the application that you want to update.					
Select a Certificate Store	Application	Certificate Assigned			
Every All Colleges All	C OS/400 TCP Central Server	None assigned			
Expand All Collapse All	C OS/400 TCP Database Server	None assigned			
▶ <u>Fast Path</u>	C OS/400 TCP Data Queue Server	None assigned			
Create Certificate	C OS/400 TCP Network Print Server	r None assigned			
<u>Create New Certificate Store</u> <u>Install Local CA Certificate on</u> Your PC	C OS/400 TCP Remote Command Server	None assigned			
Manage Certificates	C OS/400 TCP Signon Server	None assigned			
★ <u>Manage Applications</u> • View application definition	C OS/400 TCP/IP Telnet Server	None assigned			
<ul> <li><u>Update certificate assignment</u></li> <li><u>Define CA trust list</u></li> </ul>	C OS/400 DDM/DRDA Server - TCP/IP	None assigned			
<ul> <li>Add application</li> <li>Remove application</li> </ul>	C OS/400 Cluster Security	None assigned			
<ul> <li>Update application definition</li> </ul>	C OS/400 - Host Servers	None assigned			
<ul> <li>Validate application</li> </ul>	C OS/400 TCP File Server	None assigned			
Manage Certificate Store	C AS/400 Management Central Serve	r None assigned			
<ul> <li>Manage PKIX Request Location</li> </ul>	C Directory Services server	None assigned			
Return to iSeries Tasks	© OS/400 VPN Key Manager	None assigned			
Secure Connection	C OS/400 TCP/IP FTP Server	None assigned			
Jecule Connection	C Webserver Search Engine	None assigned			
	C HTTP Server Monitor	None assigned			
	O Domino	None assigned			
	C QIBM_HTTP_SERVER_ADMIN	None assigned			
	Note: Anytime you change certificate sele end your server and start it again to have t Update Certificate Assignment	ctions, you may need to the change take effect.			
<b>E</b>		🔐 Local intranet			



Now select the certificate to assign to Domino on Figure 33 and click "Assign New Certificate".



#### Figure 33

You should see the message "The certificate was assigned to the application." You are done.

This concludes the configuration of the DCM to use Domino with the 2058 Cryptographic Accelerator, or using software encryption.

Grant access to the \*SYSTEM certificate store for Domino

This step is only necessary if you did not create an application definition to use with Domino, meaning you used one that already existed.

When Domino's application definition is created in the example above, the user profile is set to QNOTES. This gives QNOTES (Domino's user profile) access to the \*SYSTEM certificate store. We need to do this manually if you did not go through that step. Enter the following commands on an OS/400 command line:

CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QNOTES) DTAAUT(\*RX)

CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QNOTES) DTAAUT(\*RX)

CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.RDB') USER(QNOTES) DTAAUT(\*RX)

If you are unsure if this is needed, go ahead and do it. This step will do no harm if the application definition already gave QNOTES access.

# 6. Configure Domino to use System SSL

# **Notes.INI Variables**

The following are the Notes.INI variables that can be set for using System SSL. The variables that have 'Y' under the "REQ?" column indicate that it is a variable that must be set in order to use System SSL.

Add the following parameters to your Domino server's Notes.ini file. Add this for each server that will be using the iSeries SSL.

NOTES.INI VARIABLE NAME	REQ?	DESCRIPTION
SYSTEM_SSL_HTTP=1	Y	Tells Domino to use the iSeries System SSL API instead of Domino's SSLPlus
		for HTTP
SYSTEM_SSL_APPLICATION_I	Y	The Application ID created in DCM for
D=DOMINO		this Domino server
SYSTEM_SSL_TIMEOUT=30000	N	The number of seconds until the SSL V3.0 session identifier expires. The range is 0-86400 (1 day) seconds. System SSL will remember SSL V3.0 session identifiers for up to this amount of time. By remembering these SSL
		V3.0 session identifiers, the amount of data exchanged during the SSL handshake can be reduced for peer applications where a complete initial handshake has already been performed. The default is 30000 seconds (8 hours)

# **Configure the Domino Server Document**

SSL must be enabled in the Domino server document. At a minimum, the SSL port will need to be enabled. Other options such as the "SSL key file name" are only used for Domino SSL tasks other than HTTP. Remember that only HTTP uses the system SSL and hardware cryptography. (Figure 34)

8 6	Server : In18b1b	1440	<b>^</b>				
	Jerver . Iprobrb/440						
	Basics Security Ports Server Tasks Internet Protocols MTAs Miscellaneou						
0	Notes Network Ports   Inter	net Ports Proxies					
61	SSL settings						
	SSL key file name:	keyfile.kyr					
3	SSL protocol version (for Negotiated use with all protocols excent HTTP):						
<b>9</b> 1	Accept SSL site certificates:	C Yes 🖲 No					
3	Accept expired SSL certificates:	⊙ Yes C No					
8 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Web Directory Mail DIIOP Remote Debug Manager						
	Web (HTTP/HTTPS)						
	TCP/IP port number:	80					
	TCP/IP port status:	Enabled					
	Enforce server access settings:	No					
	Authentication options:						
	Name & password: Yes						
	Anonymous: Yes						
	SSL port number:	443					
	SSL port status: (	Enabled					
	Authentication options:		-				

Figure 34

# 7. Configure the 2058 Cryptographic Accelerator

The 2058 Cryptographic Accelerator is simple to configure. To find the accelerator, enter the following command:

#### WRKHDWRSC \*CRP

In the result below, the 2058 Cryptographic Accelerator is resource CRP01.

Work with Cryptographic Resources

System: LP18B1B

Type options, press Enter.

5=Work with configuration descriptions 7=Display resource detail

Opt	Resource	Туре	Status	Text
	CMB05	2843	Operational	Combined function IOP
	CRPCTL03 CRP03	4758 4758	Operational Operational	Cryptographic IOA Cryptographic Device
	CRPCTL01	2058	Operational	Cryptographic IOA
	CRP01	2058	Operational	Cryptographic Device

We need to create a device description for the accelerator. Enter the following command (Substituting CRP01 for your 2058 Cryptographic Accelerator's resource name):

CRTDEVCRP DEVD(CRP01) RSRCNAME(CRP01)

38 Domino HTTP Hardware Cryptography Support using iSeries SSL

To vary on (enable) the accelerator, enter the following command: WRKCFGSTS \*DEV

Work with Configuration Status							LP18B1B
						02/02/04	15:28:40
Posit	tion to .		Starting characters				
Type options, press Enter.							
1=1	Jary on 2	2=Vary of	f 5=Work wi	ith job	8=Work with	description	
9=Display mode status			13=Work w	with APPN	status		
Opt	Descriptio	on	Status			Job	
1	CRP01		ACTIVE				
	CRP03		ACTIVE				
	DSP01		ACTIVE				
	LANTAP		VARIED OFF				
	OPT01		VARIED OFF				
	OPT02		VARIED OFF				
	QCONSOLE		VARIED OFF				
	QESPAP		VARIED OFF				
	QIADSP		VARIED OFF				
							More
Parameters or command							
===>							
		F3=Exit keys	F4=Prompt	F12=Can	cel F23=Mo	re options	F24=More

Select a 1 for 'Vary On' next to your device description, and press Enter. The device will go to ACTIVE status and you are done. All requests to the iSeries SSL will now use the 2058 Cryptographic Accelerator.

Domino HTTP Hardware Cryptography Support using iSeries SSL 39

# 8. Configure the 4758 Cryptographic Coprocessor

The 4758 Cryptographic Coprocessor is a more involved configuration process than the 2058 Cryptographic Accelerator. This document will not cover this process. The main different steps required are:

- 1. Coprocessor initialization requires the \*ADMIN HTTP server to be in SSL mode.
- 2. You must initialize the 4758 using the \*ADMIN HTTP server if not previously done.
- **3.** You must create a new certificate for Domino that uses 'hardware' or 'hardware encryption' for key storage rather than software (selected during certificate creation).

Under V5R2, see the topic e-business and Web serving->Web Serving->Set up->Set up SSL for the ADMIN Server (powered by Apache) in the iSeries Information Center for information on configuring the \*ADMIN HTTP server to use SSL.

http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/rzaie/rzaieconfigssladmin.htm

See chapters 3.2.4 to 3.2.6 for information on configuring the 4758 Cryptographic Coprocessor in the Redbook "iNotes Web Access on the IBM eServer iSeries Server." This Redbook was written for Domino usage of the coprocessor and is recommended.

http://www.redbooks.ibm.com/redbooks/pdfs/sg246553.pdf

See the topic Security->4758 PCI Cryptographic Coprocessor for iSeries in the iSeries Information Center for information on configuring and using the 4758 Cryptographic Coprocessor.

http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/rzajc/rzajcco4758.htm

The Redbook "IBM  $\sim$  iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptography Enhancements" contains step-by-step instructions of configuring the 4758, as well as creating a certificate that will use it. See Chapter 4 of the Redbook for details. Appendix C also contains information on configuring the \*ADMIN HTTP server for SSL.

http://www.redbooks.ibm.com/redbooks/pdfs/sg246168.pdf

#### **Additional Information:**

iSeries Information Center: V5R2->Networking->Networking security->Cryptographic hardware

Contains links to configuration information of the 4758 and 2058 accelerators.

http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/rzajc/rzajcoverview.htm