

Digital Certificate Manager Setup

Contents	Page
Pre-configuration	3
Sample control scripts	3
Server Requirements	3
Prerequisites	3
Technical documents available online at	3
Firewall Considerations	4
Introduction	5
1. Problem Overview	5
2. Problem Definition	5
3. Solution	5
Configuration	6
4. Configure iSeries Servers to use FTP *Secure	6
5. SERVER1 home server: Setup DCM tasks	9
6. Select Digital Certificate Manager	10
7. Create a Certificate Authority	11
8. Install a local Certificate Authority certificate	11
9. Certificate Authority (CA) Policy Data	12
10. Create the *SYSTEM certificate store and server certificate	14
11. Select Applications	15
12. Configure the FTP Server to listen for secure connections	17
13. Restart the FTP Server	18
14. Export local Certificate Authority	19
15. Transport certificates to partnering servers	21
16. Import the CA certificate - from the Digital Certificate Manager	22
17. Configure FTP client to trust Certificate Authority from partnering server	22
Test the configuration	23
18. Start a successful secure FTP session to the remote server	23
19. Start a secure FTP session to remote server with a certificate disabled	24
Change original configuration	25
20. Limit FTP access to a specific server:	25
21. Sample scripts provided	26

Appendix A:	Security Procedure Tips	27
Appendix B:	Terms associated with digital certificates	28
Appendix C:	How to move certificates between servers	29
Appendix D:	Sample scripts	31
Appendix E:	Batch FTP *Secure command parameters	34
Appendix F:	Restart the security definition process	36

Pre-configuration

Sample control scripts

Network ID: *FTP_EXTOL: Portal/Easy Link scripts: RCVSSL – Receive via SSL; SENDSSLEDI – Send EDI data via SSL; SENDSSLTXT – Send TXT data via SSL.

Other sample scripts: SEND_SECUR – Send to IFS Folder w/SSL; SEND_SECU2 – Send to IP Address w/SSL.

Server Requirements

- iSeries with V5R2 or later of OS400.
- V5R2 or later of TCP/IP Connectivity Utilities (5722-TC1).
- Cryptographic Access Provider 128-bit for iSeries (5722-AC3).
- IBM Digital Certificate Manager DCM (5722-SS1, Option 34).
- IBM HTTP Server (5722-DG1).
- The home server uses Certificates to protect access to public applications.
- All servers use OS400 TCP/IP FTP server/client for FTP sessions.
- EXTOL EDI Integrator V 6.1 or greater (to utilize the BATCHFTPS command).

With security officer authority – review the installed programs on the iSeries server.

At a command line, type:go licpgm, select option #10 - Display installed licensed programs, ensure the Installed status is either *COMPATIBLE or *INSTALLED and the option is satisfied. Press F11 to toggle the display.

Prerequisites

- All software requirements for working with SSL on iSeries are installed.
- The ***ADMIN HTTP** instance is started on both iSeries servers for the use of Digital Certificate Manager (DCM).
- User profiles performing all configurations have ***IOSYSCFTG** special authority.
- A Certificate Authority or *SYSTEM store has not been created on either system.

Technical documents available online at

• Digital Certificate Infrastructure:

o http://www.redbooks.ibm.com/redbooks/pdfs/sg245659.pdf

- V5 TCP/IP Applications:
 <u>http://www.redbooks.ibm.com/redbooks/pdfs/sg246321.pdf</u>
- IBM eServer iSeries Wired Network Security
 - o http://www.redbooks.ibm.com/redbooks/pdfs/sg246168.pdf
- V4 TCP/IP for AS/400: More Cool Things Than Ever
 - o http://www.redbooks.ibm.com/redbooks/pdfs/sg245190.pdf
- For security terminology see Appendix A.

Firewall Considerations

• Symantec – Passing outbound SSL – secured:

<u>http://service1.symantec.com/SUPPORT/ent-</u> gate.nsf/805bf841a2655e7988256d9700455b6c/971a36a467b670328825708c00531d09?OpenDocumen t&src=bar_sch_nam&seg=en

Important: Every firewall has unique configuration requirements. It is recommended that the Firewall-specific Support Team is notified with the intended communication plans prior to actively exchanging data using FTP *Secure.

Introduction

1. Problem Overview

Two iSeries servers must communicate via FTP with secure active (SSL).

2. Problem Definition

Two iSeries servers must communicate via FTP with *Secure. The home server is located in New Jersey with the system name SERVER1. The remote server is located in Pennsylvania with a system name SERVER2. In each location there is an iSeries used to run various business applications. Each night the remote server in PA, SERVER2, is required to send reports to the main headquarters in New Jersey, SERVER1. Until now the files were simply transferred files over the Internet using FTP. The customer is now looking for a solution that will move the files with privacy and security intact from SERVER2 to SERVER1, in both directions.

3. Solution

The solution to this problem would be to use the home box, SERVER1, as the FTP Server and the remote box, SERVER2, as the FTP Client. This same solution would apply for multiple remote locations.

In order to use SSL secured FTP sessions, the FTP server must have a certificate associated with it. Also, the FTP client(s) must trust the Certificate Authority (CA) that issued the FTP server's certificate. In this scenario we use a local Certificate Authority to issue the server's certificate. The Certificate Authority is created on the iSeries server in New Jersey, SERVER1.

Important: EXTOL provides this working example for this particular scenario of security requirements. This is a sample solution and as such should be used as a guide. Installation plans should be made prior to starting the security setup. It is up to the installer to adjust security requirements as applicable.

Configuration

•

4. Configure iSeries Servers to use FTP *Secure

For both SERVER1 & SERVER2 servers:

- Plan the configuration of:
 - Local certificate authority
 - System store and server certificate
 - Create the local certificate authority
- Create the *SYSTEM server certificate
- Configure the FTP server to listen for secure connections
- Export the certificate of authority to the IFS

Transport Certificates: Transport certificate(s) as needed

SERVER2: Remote server

• Import the Certificate Authority certificate from SERVER1 into *SYSTEM certificate store

SERVER1: Home Server

- Import the certificate of authority from other server into *SYSTEM certificate store.
- Configure the FTP client to trust the SERVER2 certificate authority.

Test configuration.

SETUP / PLANNING STEPS FOR CERTIFICATE CREATION

4.1.a Certificate Authority Configuration – Plan values for SERVER1 & SERVER2

	SERVER1 (NJ)	SERVER2 (PA)
CONFIGURATION	PARM VALUE	PARM VALUE
Key size	1024	1024
Certificate Authority name	EXTOL Inc. SERVER1 CA	EXTOL Inc. SERVER2 CA
Organization unit	New Jersey Headquarters	PA Office
Organization name	Extol Inc.	Extol Inc.
Locality	Franklin Lakes	Pottsville
State	New Jersey	Pennsylvania
Country	US	US
Validity period of Certificate	1095 (default)	1095
Allow creation of user certs	NO	NO
Verify period of certificates issued		
By the CA (default=365)	365 days	365 days

4.1.b *SYSTEM server configuration: The FTP server needs a server certificate in order to create secure connections with the FTP clients.

	SERVER1 (NJ)	SERVER2 (PA)	
CONFIGURATION	PARM VALUE	PARM VALUE	
Key size	1024	1024	
Certificate label	SERVER1 FTP Server	SERVER2 FTP Server	
Common name	SERVER1 FTP Server	SERVER2 FTP Server	
Organization unit	New Jersey Headquarters PA Office		
Organization name	Extol Inc.	Extol Inc.	
Locality	New Jersey	Pottsville	
State	New Jersey	Pennsylvania	
Country	US	US	

SETUP OF iSeries Digital Certificate Manager certificates:

ALL: Ensure the HTTP server is started:

- 1. WRKACTJOB SBS(QHTTPSVR)
 - You should see several jobs named ADMIN running in this subsystem.
 - a. To start the server:
 - STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
 - ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

Verify the jobs start. If this is the first time the ADMIN server is started it may take several minutes before you may access it. Proceed to the next step once you verify that all of the ADMIN jobs (there should be 3) have started and are in **SIGW** status.

To setup multiple servers – execute steps a through k for each system.

- (a) Log on to server with iSeries task menu
- (b) Click on Digital Certificate Manager
- (c) Create a certificate authority
- (d) Install local CA certificate authority
- (e) The certificate authority policy data
- (f) Create a *System certificate store and server certificate.
- (g) Select applications
- (h) Configure the FTP server to listen for secure connections
- (i) Restart FTP server
- (j) Export local CA for exchange
- (k) Transport certificate to partnering server and rename to extension: .cer.
- Do each of the following for each server:
 - o (I) Import the local certificate authority to partnering server
 - (m) Configure FTP client to trust the imported certificate

5. SERVER1 home server: Setup DCM tasks

Access the iSeries Task page by opening the location http://SERVER1:2001/ or http://SERVER2:2001/

Sign on to server with Security officer authority.



6. Select Digital Certificate Manager

<page-header><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image><image>

On the iSeries Task page, click Digital Certificate Manager.

On the DCM page, in the navigation (left) panel, click on Create a Certificate Authority (CA).

Note: Tip: If you do not see the *Create a Certificate Authority* option in the left panel you already have a local Certificate Authority on this system. Reference the Redbook AS/400 Internet Security: Developing a Digital Certificate Infrastructure, SG24-5659-00 for information on deleting the Certificate Authority and store. Section 5.2.3 gives the name and location of all of the files that make up the Certificate Authority and *System certificate store. These files can be deleted allowing you to start from scratch. Prior to deleting the *System store you should verify that the store does not contain certificates that have been purchased or are currently in use. *There is no way to recover files that have not been backed up after performing this operation.*



7. Create a Certificate Authority

Reference values declared in Table 4.1.b, page 7:

- Key Size default is 1024
- Assign password for local Certificate of Authority.
- Certificate Authority (CA) name
- Organization unit
- Organization name
- Locality or city, State, Country or Region
- Validity period of Certificate Authority
- Click Continue.

Note: If the Local CA has already been created - you will see:

"Install Local CA Certificate on Your PC" - if so, skip this step.

8. Install a local Certificate Authority certificate

If you want your browser to trust the local Certificate Authority, you must add the local CA certificate to the browser configuration. To add the CA certificate, click **Install certificate** and follow the steps. This is not a required step but may be useful if you ever plan on using this CA certificate to secure browser based applications.

Click Continue.

	Digital Certificate Manager 🛛 🛛 IEM.
	Install Local CA Certificate
And a source of the source of	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.
▶ <u>Manage User Certificates</u>	You must install the Certificate Authority (CA) certificate in your browser so the
<u>Create New Certificate Store</u> <u>Create a Certificate Authority</u> (CA)	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.
► Manage CRL Locations	Install certificate
<u>Manage LDAP Location</u> <u>Manage PKIX Request Location</u> <u>Return to iSeries Tasks</u>	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).
Secure Connection	Continue Cancel

9. Certificate Authority (CA) Policy Data

Allow creation of user certificates? Default is No.

Validity period of certificates that are issued by this Certificate Authority (CA) field specify the number of days the certificates issued by the local CA are valid.

Click Continue.

	Digital Certificate Ma	nager	0 IEM.	
	Certificate Authority (CA) Policy Data			
Care States	Your Certificate Authority (CA) was created with the default policy data shown below. Change the data if you want and then select Continue.			
Select a Certificate Store	Allow creation of user certificates:	🔿 Yes	⊙No	
Expand All Collapse All	Validity period of certificates that are issued by this Certificate Authority (CA) (1-2000):	l 365 (days)		
 Manage User Certificates Create New Certificate Store 	Days until Certificate Authority (CA) expires: 109	95		
 <u>Create a Certificate Authority</u> (<u>CA</u>) 	Continue			
▶ <u>Manage CRL Locations</u>				
 Manage LDAP Location 				
 Manage PKIX Request Location 				
<u>Return to iSeries Tasks</u>				
Secure Connection				

The creation of the Certificate Authority is now complete. Select **Continue**. You can now begin creating the *SYSTEM certificate store and server certificate.

	Digital Certificate Manager 🛛 🛛 IEM.
	Policy Data Accepted
A CONTRACTOR OF CONTRACTOR	Message The policy data for the Certificate Authority (CA) was accepted.
Select a Certificate Store	Select Continue to create the default server certificate store (*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.
Expand All Collapse All	
▶ <u>Manage User Certificates</u>	Continue
Create New Certificate Store	
<u>Create a Certificate Authority</u> <u>(CA)</u>	
▶ Manage CRL Locations	
Manage LDAP Location	
Manage PKIX Request Location	
Return to iSeries Tasks	
Secure Connection	

10. Create the *SYSTEM certificate store and server certificate

The *SYSTEM certificate store maintains the server certificate associated with the FTP server. If you have never created certificates on this system the *SYSTEM store will not exist.

- Key Size (default value 1024)
- Certificate Label
- Certificate store password (record for future use)
- Common Name
- Organization, locality, state, and country
- Click Continue.

Message Your certificate was created and placed in the *SYSTEM certificate store.				
	Digital Certificate Manager Select Applications Message Your certificate was created and placed in the *SYSTEM certificate store.			
Select a Certificate Store Expand All Collapse All Manage User Certificates Create New Certificate Store	Certificate type: Server or client Certificate store: *SYSTEM Select which applications will use this certificate:			
Create a Certificate Authority (CA) Manage CRL Locations Manage LDAP Location Manage PKIX Request Location Return to iSeries Tasks	Warning: When you assign a certificate to a client application and a server requests client authentication, then the server authenticates all users of the application based on that certificate. Consequently, the server does not authenticate users on an individual basis. To ensure that the server authenticates each user of a client application individually outside the SSL protocol, do not assign a certificate to the client application.			
Secure Connection	Select All Clear All			

11. Select Applications

Scroll down and *check* OS/400 TCP/IP FTP Server.

Click Continue.

		Digital Certificate M	[anag	er 🛛 🛛	IBM⊗
		OS/400 DDM/DRDA Server - TCP/IP	Server	(None assigned)	<u>^</u>
Car Clina Internetion		OS/400 Cluster Security	Server	(None assigned)	
All Balling		OS/400 - Host Servers	Server	(None assigned)	
Select a Certificate Store		OS/400 TCP File Server	Server	(None assigned)	
		Management Central Server	Server	(None assigned)	
Expand All Collapse All		IBM Directory Server	Server	(None assigned)	
▶ Manage User Certificates		IBM Directory Server publishing	Client	(None assigned)	
<u>Create New Certificate Store</u>		IBM Directory Server client	Client	(None assigned)	
<u>Create a Certificate Authority</u>		OS/400 VPN Key Manager	Server	(None assigned)	
Manage CRL Locations		Enterprise Identity Mapping (EIM)	Client	(None assigned)	
Manage LDAP Location		Webserver Search Engine	Server	(None assigned)	
Manage PKIX Request Location		HTTP Server Monitor	Server	(None assigned)	
Return to iSeries Tasks		OS/400 TCP/IP FTP Server	Server	(None assigned)	=
Secure Connection		OS/400 TCP/IP FTP Client	Client	(None assigned)	
	Cc	ntinue Cancel			~

When the application status is successful - click **Cancel**.

	Digital Certificate Manager 🛛 🛛 IBM.
	Application Status Message The applications you selected will use this certificate.
Expand All Collapse All	Select Continue to create the default object signing certificate store (*OBJECTSIGNING) and an object signing certificate signed by your Certificate Authority (CA). You can then use your system to sign objects.
 Manage User Certificates Create New Certificate Store Create a Certificate Authority (CA) Manage CRL Locations Manage LDAP Location Manage PKIX Request Location Return to iSeries Tasks Secure Connection 	Continue Cancel

12. Configure the FTP Server to listen for secure connections

From the iSeries Navigator:

- Expand iSeries server
- Expand Network
- Expand Servers
- Click on TCP/IP
- Right click on FTP and select Properties

🤨 iSeries Navigator			
File Edit View Help			
🧈 🕨 🕘 🖂 🖆 🖓 🚺 🛇			1 minutes old
Environment: My Connections	Exdev: TCP/IP		
🖅 📳 Management Central (Exdev)	Server Name	Status	Description
🖻 🏥 My Connections	The INETD	Stopped	INETD
🖻 📲 Exdev	The EDRSQL	Stopped	Extended Dynamic Remot
Basic Operations	The SNTP	Stopped	SNTP
🕀 🛅 Work Management	- Radio Cos	Stopped	Quality of Service
Configuration and Service	RADIUS NAS	None	RADIUS Network Access S
	RebFacing	Started	WebFacing server
CP/IP Configuration	📅 System Debug	Stopped	Graphical system debug s
Remote Access Services	Management Central	Started	Management Central
		Stopped	Datalinks File Server
	📅 Virtual Private Networking	Stopped	Virtual private networking
DNS	To ASFTomcat	Started	ASFTomcat server
Liser-Defined	Triggered Cache Manager	Stopped	Triggered cache manager
+ Policies	ToFT Shart	Started	FTP
🕂 🧱 Windows Administration		Started	LPD 🔜
< >	Stop		>
	Server Jobs		
 My Lasks - Exdev Add a connection ✓ Install additional components 	Create a new DNS Name S	rver jobs 📅 Cor erver 🕨 ? Hel server	nfigure system as Directory server (p for related tasks
Displays the properties of the selected items.			

For the **General** tab's **Sockets layer support to be started with the server** option, select either **Secure Only** or **Both Secure and Non-secure** (Default).

Click OK.

😤 FTP Properties - Exdev		
General Mappings Initial Formats		
Start when TCP/IP is started		
Initial number of servers to start (1 - 20):	3	
Inactivity timeout:	3600 seconds	
Subsystem:		
O Use default (QSYS/QSYSWRK)		
C Subsystem description:		-
Library:		ī
Sockets layer support to be started with server:		
C Secure only		
O Non-secure only		
Both secure and non-secure		
	OK Cancel	Help ?

13. Restart the FTP Server

In order for the modifications to take effect, the FTP server should be restarted. Once this done the FTP server will be able to support secure connects with any clients that trust our Certificate Authority. (See Security Procedure Tips – "To start and stop the TCP Server")

This completes the configuration of the FTP server to accept secure connections.

14. Export local Certificate Authority

Export the local certificate authority certificate to IFS (for iSeries partnering machine)

- To establish the trust between servers the home server exports the local CA certificate to be imported on the remote server. The FTP client on the remote server must trust the local Certificate Authority that signed the FTP server certificate.
 - o Click on Select a Certificate Store button
 - o Select the Local Certificate Authority (CA) button, click Continue
 - o Enter password and click Continue
 - o Expand the Manage Local CA and click on Export, click Continue

	Digital Certificate Manager 🛛 🛛 IBM.
	Manage Local Certificate Authority (CA)
Contraction of the second seco	Select the type of action that you want to perform.
	 View - View information pertaining to a certificate.
Select a Certificate Store	• Renew - Replace your existing local Certificate Authority (CA) certificate with a new certificate.
Expand All Collapse All	 Export - Copy your local Certificate Authority (CA) certificate to a file or to another certificate store.
<u>Create Certificate</u>	🔿 Delete - Delete your local CA.
Create New Certificate Store	Change policy data - Change the policy data for your local CA.
 Install Local CA Certificate on Your PC 	 Change password - Change the password for your local CA.
▶ <u>Manage User Certificates</u>	Cantinua
▼ <u>Manage Local CA</u> ■ <u>View</u>	
• <u>Renew</u>	
■ <u>Export</u> ■ Delete	
Change policy data	
 Change password 	
▶ Manage CRL Locations	
- M	

- o Select File (radio button) and click Continue
- o Supply the Export file name to the IFS, click Continue
- It is suggested that a standard IFS folder is created for all certificates. The example here is /cert.



- 1. Sample: /cert/i5p1ca.cer
 - a. For this example "Cert" is the Folder Name.
- 2. Confirmation message and click OK
 - a. The contents of this message vary based on release.

Export Certificate Successful

Message	The Certificate Authority (CA) certificate was successfully copied to the export file:
	/Cert/i5p1ca.cer
	You must now transfer the file to the system that will use this Certificate Authority (CA) certificate.
ОК	

15. Transport certificates to partnering servers

See Appendix C for available options.



16. Import the CA certificate - from the Digital Certificate Manager

- Click on Select a certificate store button
 - Select the ***SYSTEM** radio button, click **Continue**
 - Supply the password, click **Continue**
 - o Expand Manage Certificates and select Import Certificate
 - Select the Certificate Authority (CA) radio button and click Continue
 - o Import Certificate select Certificate Authority (CA), click Continue
 - Supply the path and file name of the certificate authority (CA) and click Continue
 - o /cert/SERVER1CA.cer, press Enter
 - Provide the **CA Certificate Label** by:
 - i. Provide your desired description or if you prefer to use what the value was on file:
 - 1. Return to the Certificate Authority View
 - 2. Highlight and copy the Certificate label:
 - LOCAL_CERTIFICATE_AUTHORITY(1)
 - 3. Paste copied value into the CA Certificate Label, click Continue
 - ii. You should receive the following message:

Import Certificate Authority (CA) Certificate

Mess	e The certificate has been imported.	
	Use the Manage Applications task if you want to specify that applications trust this Certificate Authority (CA).	Ð
ОК		

Click OK.

17. Configure FTP client to trust Certificate Authority from partnering server

- After the certificate is imported expand Manage Applications
- Click on **Define CA trust List**.
- Click the **Client** radio button, click **Continue**
- Select the OS/400 TCP/IP FTP Client radio button and click Define CA Trust List
- A list of certificate authorities is displayed.
 - Select the recently imported CA in the **Trusted** column and click **OK**.
 - Select the Local CA from server and check the **Trusted** column. Click **OK**.
- The list will be redisplayed with the change in place. The following message will be displayed: "Certificate Authority (CA) changes applied".

Message Certificate Authority (CA) changes applied.

Click Cancel to exit.

Test the configuration

18. Start a successful secure FTP session to the remote server

At a command line, type: FTP RMTSYS(SERVER1) PORT(*SECURE)

Press Enter.



19. Start a secure FTP session to remote server with a certificate disabled

At a command line, type: FTP RMTSYS(SERVER1) PORT(*SECURE)

Press Enter.



To disable a certificate, see step 20.

Change original configuration

20. Limit FTP access to a specific server:

To turn on / off Trusted certificates

- Visit ***System** certificate store on home server
- Select Set CA Trust
- Define partnering certificate to **Disallow** and confirm
 - This will cause an ftp communication to fail from home server (return code –23) but the partnering server can still connect with *Secure.
- Test configuration.

If **Disallowed** partnering local CA – and wish to reactivate it's secure permission:

- Must revisit to Allow the Trusted status
- Revisit the FTP server and client to ensure the certificates are trusted.
- This is proven by retesting your scripts to connect properly.

Important: As certificates are changed, disallowed, or imported into the DCM security bank, manual records should be kept offline for emergency recovery purposes.

21. Sample scripts provided

Batch FTP with Secure (V5R2) (BATCHFTPS) File Edit Functions Help Remote system Name Override INPUT to file Name, *LIBL, *CURLIB *LIBL Library ***FIRST** Name, *FIRST, *LAST Override INPUT to member *NONE Name, *NONE Override OUTPUT to file Name, *LIBL, *CURLIB Library ***FIRST** Name, *FIRST, *LAST Override OUTPUT to member Internet address 1-65535, *DFT, *SECURE *DFT Port *DFT *DFT, *IMPLICIT, *SSL, *NONE Secure Connection * 0K Cancel Help IBM 3

Screen Layout for Batch FTP command with Secure:

Sample of Batch FTP with Secure active within control script: CCMDEXC CMD(BATCHFTPS RMTSYS(loopback) INPUTFILE(@NL+ /QTXTSRC) INPUTMER(I@CL) OUTPUTFILE(@NL/QT+

/QTXTSRC) INPOTMBR(I@CL) OUTPOTFILE(@NL/QT+ XTSRC) QUIPUIMBR(O@CL) PORT(*SECURE) SECCN+ N(*DFT) DTAPROT(*DFT))

Appendix A: Security Procedure Tips

Start and stop the TCP Server

- To ensure all changes are effective the TCP server may need shutdown and restarted.
 - Check active jobs to ensure TCP server is running:
 - WRKACTJOB SBS(QHTTPSVR)
 - There should be a few ADMIN, QTMHHTTP jobs running.
 - To manually start: STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
 - To manually end: ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

Other

You can specify another directory such as /your_directory_name to store certificates. Customer applications that are written to use SSL_Init (instead of the newer SSL_Init_App) can make more use of this. System administrators can also make use of this certificate store for certain kinds of backups or testing before moving into their production environment. Some functions, such as exporting certificates from certificate stores created while the system was on a previous release, may also make use of this. Again do not use this if you want to use OS/400 secure applications.

Appendix B: Terms associated with digital certificates

Authentication

Authentication is the function of proving the identity of an entity.

AS/400 DCM

The AS/400 Digital Certificate Manager (DCM) is an application for managing digital certificates. It includes the ability to create and store certificates on the AS/400, to validate certificates, and to associate certificates with user profiles and applications.

Certificate Authority (CA)

A CA is an organization that issues digital certificates. Companies such as VeriSign and Thawte are examples of Internet Certificate Authorities. A digital certificate will be issued from a Certificate Authority when the required information is given to them, a fee is paid, and the information passes their security checks.

Digital Certificates

A digital certificate is a form of personal identification that can be verified electronically. It is used as a form of identification for individual persons and other entities, such as servers. A digital certificate can be compared with a passport. The issuing bureau validates the authenticity of the data in a passport. A certificate authority (CA) issues digital certificates and validates them as well.

Digital certificates can be used for authentication, for convenience, to secure information being transmitted across a not trusted network, and to establish the ownership and integrity of information you receive.

Entity

An entity is a person, organization, or machine that can participate in a communications network.

Secure transmitted data

Digital certificates are used as the basis for Secured Socket Layer (SSL), which is a method of encrypting data sent across TCP/IP networks. SSL can be used by most of the services that run across TCP/IP to ensure others cannot intercept or modify data.

NOTE: To establish a secure SSL connection, only the server needs to possess a certificate.

HTTP servers frequently use SSL, and generally the client browsers do not possess a certificate. However, the CA that signed the HTTP server's certificate must be known to the client browsers.

Appendix C: How to move certificates between servers

To distribute local certificate authority(s) to partnering servers from Windows

- From the home server:
 - o Select a certificate store, Local Certificate Authority (CA), enter password
 - Select Install Local CA Certificate on Your PC
 - o Select Copy and Paste
 - Copy the entire certificate from BEGIN CERTIFICATE through END CERTIFICATE-----
 - Launch the Notepad application. Paste the Certificate information with the "Courier" font.
 - Save the Notepad document to your Desktop. There are no specific rules on naming conventions but a suggestion would be: SERVER1CA.cer.
 - To distribute: To ship by email the file may need to be renamed .cert to allow electronic transfer.

If transporting a certificate that was exported to IFS (binary format)

a. Using OS/400 operating system tools:

Note that the following instructions only describe a summary of steps and not the details because basic OS/400 knowledge is presumed. To move this export file from the source to the target system, follow these instructions:

- Create a save file (SAVF).
- Save the export file from the IFS using the SAV command into the SAVF.
- Transfer the SAVF to the target system.
- Restore the export file to the IFS using the RST command.

We recommend the approach described here to transfer the CA certificate using a save file. If you use FTP to transfer the export file directly, this can cause the error Base64 encode error when receiving the CA certificate on the target system. This error occurs when you use the wrong format when FTPing the file.

SAV DEV('\QSYS.LIB\EXTSAVF.LIB\DCMCERT.file') OBJ(('/DSMITH/SERVER1CA.cer'))

b. Using OS/400 FTP to retrieve exported certificate from IFS:

From iSeries server green screen:

FTP	SER	VEF	21		
User	Id	(QI	DSMI	TH)
Pass	swor	d (QSPI	EEDY)
NAME	FMT	' 1			
CD /	'DSM	ITH	I		
LCD	/DS	МІЛ	Ή		
GET	SER	VEF	R1CA	.cer	
QUIT	-				

c. Using WS_FTPLE tool:

- Start up: WS_FTPLE 95
- Connect to local server (SERVER1) in your local folder
- Transfer the SERVER1CA.cer in ASCII mode to your local folder
- Close the connection from the local server (SERVER1)
- Reconnect to the remote server (SERVER2)
- Transfer the exported CA from your local folder to the remote server folder
 - o From /local folder
 - o To /SERVER2/Your IFS Folder
- Close the connection with the remote server (SERVER2)
 - To view your transferred file use windows explorer
 - o Drill down to your local folder on SERVER2
- Right click on the exported certificate (SERVER1CA.cer)
- Select: Open with
- Roll cursor down to WordPad and select
 - o The exported file should resemble this following layout:

⁻⁻⁻⁻BEGIN CERTIFICATE-----

MIICIDCCAYmgAwIBAgIEQ6C0ZjANBgkqhkiG9w0BAQQFADBKMQswCQYDVQQGEwJV UZETMBEGA1UECBMKTmV3IEplcnNleTETMBEGA1UEChMKRVhUT0wgSW5jLjERMA8G A1UEAxMIRVhUUk4gQ0EwHhcNMDUxMjE0MDAxMDE0WhcNMDgxMjE0MDAxMDE0WjBK MQswCQYDVQQGEwJVUZETMBEGA1UECBMKTmV3IEplcnNleTETMBEGA1UEChMKRVhU T0wgSW5jLjERMA8GA1UEAxMIRVhUUk4gQ0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0A MIGJAoGBAL8FNFfDIxAgaXduA8qKai8pFNUnvA8Z67Xh3muuBU4aoxbzN3EGbjzH AAR4I0jZzapbSf9P9oh/ZORbfAu0bnfdIbSQ203nT87LBP004otixSZ6vWc+9dpc D5rpvQUCkJg6TH+xWf3LDD5C5L1vGr0oc7+WGmx7Cg23Scdc88BhAgMBAAGjEZAR MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAtDh/h5Nr/w+i239W OB450g8ALhsjt1AXI8GCP2JnaEA1TN+qJdVmy/MVwp+pgZTJyO5t+cUwC5G8g7w/ VYuuSQ5RqNnos71kUMXmLL+PUIK/iesB2LP8jmNenOY7H82heLJphLSrrJj6yfsM 3I+LvzTY+tbFeMcMx+R+nFb4yn8=

⁻⁻⁻⁻END CERTIFICATE-----

Appendix D: Sample scripts

Network: *FTP_EXTOL, Control Script: RECVSSL

- CWRTLINE LINEDATA('account password')
 - CWRTLINE LINEDATA('namefmt 1')
 - CWRTLINE LINEDATA('Icd /folder/inssl')
 - CWRTLINE LINEDATA('bin')
 - CWRTLINE LINEDATA('mget *')
 - CWRTLINE LINEDATA('quit')
 - CSETUP CLOSE(*YES)
 - CCMDEXC CMD(DLTOVR FILE(QTXTSRC))
 - CCMDEXC CMD(BATCHFTPS RMTSYS(SFTP.EASYLINK.COM) INPU+ TFILE(@NL/QTXTSRC) INPUTMBR(I@CL) OUTPUTFI+ LE(@NL/QTXTSRC) OUTPUTMBR(O@CL) POR+ T(61476) SECCNN(*SSL) DTAPROT(*DFT))
 - CCMDEXC CMD(SCANTXTSRC SCANSTRING(*MSGID) FILE(@NL/Q+ TXTSRC) MBR(O@CL) MSGQ(C@CL) MSGF(*LIBL/EX+ TSSL) MSGID(MSG0001 MSG0002) IGN+ ORECASE(*YES) ERRCON(*ABSENT))

CCMDEXC CMD(PRCDIRSF FROMDIR('/folder/inssl') OPTION(*CMBDLT)+ TOMBR('/QSYS.L-

- IB/@NL.LIB/@NC.FILE/T@CL.MBR') TAB+ EXPN(*NO) MBROPT(*ADD) ENDLINFMT(*FIXED))
 - CCMDEXC CMD(CPYF FROMFILE(@NL/@NC) TOFILE(@NL/@NC) F+ ROMMBR(@ND) TOMBR(R@CL) MBROPT(*REPLACE))
 - CCMDEXC CMD(CPYF FROMFILE(@NL/@NC) TOFILE(@NL/@NC) F+ ROMMBR(T@CL) TOMBR(R@CL) MBROPT(*ADD))
 - CCMDEXC CMD(CRTCNNIMP FILE(@NL/@NC) MBR(R@CL) FROMCH+ AR(1) TOCHAR(@NR) SCRIPT(@CS) CNNLOGNBR(@C+ L) UPDATELOG(*PREV) IMPORTSCR(*NONE) FOR+ MAT(*WRAP))
 - CCMDEXC CMD(CPYSRCF FROMFILE(@NL/QTXTSRC) TOFILE(*PR+ INT) FROMMBR(I@CL))
 - CCMDEXC CMD(CPYSRCF FROMFILE(@NL/QTXTSRC) TOFILE(*PR+ INT) FROMMBR(O@CL))
 - CCMDEXC CMD(RMVM FILE(@NL/QTXTSRC) MBR(I@CL))
 - CCMDEXC CMD(RMVM FILE(@NL/QTXTSRC) MBR(O@CL))
 - CCMDEXC CMD(RMVM FILE(@NL/@NC) MBR(T@CL))
 - CCMDEXC CMD(RMVM FILE(@NL/@NC) MBR(R@CL))

CEXIT

Network: *FTP_EXTOL, Control Script: SEND_SECUR

```
CCMDEXC CMD(ADDMBR MBR(I@CL) PFILE(@NL/QTXTSRC) MBRO+
PT(*REPLACE) TEXT('@CS/@NP JOB:@JN/@JU/@JB-
```

'))

CCMDEXC CMD(ADDMBR MBR(O@CL) PFILE(@NL/QTXTSRC) MBRO+ PT(*REPLACE) TEXT('@CS/@NP JOB:@JN/@JU/@JB-

'))

CCMDEXC CMD(OVRDBF FILE(QTXTSRC) TOFILE(@NL/QTXTSRC) + MBR(I@CL))

CSETUP OPEN(*YES)

CWRTLINE LINEDATA('account password')

CWRTLINE LINEDATA('NAMEFMT 1')

CWRTLINE LINEDATA('CD /dsmith/edidata')

CWRTLINE LINEDATA('LCD /QSYS.LIB/@NL.LIB')

- CWRTLINE LINEDATA('PUT @NC.FILE/@ND.MBR C@CL.Edi')
- CWRTLINE LINEDATA('DIR')
- CWRTLINE LINEDATA('QUIT')
- CSETUP CLOSE(*YES)
- CCMDEXC CMD(DLTOVR FILE(QTXTSRC))
- CCMDEXC CMD(BATCHFTPS RMTSYS(loopback) INPUTFILE(@NL+ /QTXTSRC) INPUTMBR(I@CL) OUTPUTFILE(@NL/QT+ XTSRC) OUTPUTMBR(O@CL) PORT(*SECURE) SECCN+ N(*DFT) DTAPROT(*DFT))

CEXIT

Network: *FTP_EXTOL, Control Script: SEND_SECU2

```
CCMDEXC CMD(ADDMBR MBR(I@CL) PFILE(@NL/QTXTSRC) MBRO+
PT(*REPLACE) TEXT('@CS/@NP JOB:@JN/@JU/@JB-
```

```
'))
```

```
CCMDEXC CMD(ADDMBR MBR(O@CL) PFILE(@NL/QTXTSRC) MBRO+
PT(*REPLACE) TEXT('@CS/@NP JOB:@JN/@JU/@JB-
```

'))

- CCMDEXC CMD(OVRDBF FILE(QTXTSRC) TOFILE(@NL/QTXTSRC) + MBR(I@CL))
- CSETUP OPEN(*YES)
- CWRTLINE LINEDATA('account password')
- CWRTLINE LINEDATA('close')
- CWRTLINE LINEDATA('SOpen '172.x.x.')
- CWRTLINE LINEDATA('user name password')
- CWRTLINE LINEDATA('NAMEFMT 1')
- CWRTLINE LINEDATA('CD /dsmith')
- CWRTLINE LINEDATA('LCD /QSYS.LIB/@NL.LIB')
- CWRTLINE LINEDATA('PUT @NC.FILE/@ND.MBR')
- CWRTLINE LINEDATA('DIR')
- CWRTLINE LINEDATA('QUIT')
- CSETUP CLOSE(*YES)
- CCMDEXC CMD(DLTOVR FILE(QTXTSRC))
- CNOOP TEXTSTRING('ECCNN(*DFT) DTAPROT(*DFT) +
 ')
- CCMDEXC CMD(BATCHFTP RMTSYS(loopback) INPUTFILE(@NL/+ QTXTSRC) INPUTMBR(I@CL) OUTPUTFILE(@NL/QTX+ TSRC) OUTPUTMBR(O@CL))

CEXIT

Batch FTP with Secure (V5R2) (B	ATCHFTPS)	
File Ealt Functions Help		
Remote system	>	
Override INPUT to file	>	Name
Library	*LIBL	Name, *LIBL, *CURLIB
Override INPUT to member	FIRST	Name, *FIRST, *LAST
Override OUTPUT to file	NONE	Name, *NONE
Library		Name, *LIBL, *CURLIB
Override OUTPUT to member	FIRST	Name, *FIRST, *LAST
Port	> SECURE	1-65535, *DFT, *SECURE
Secure Connection	*DFT	*DFT, *IMPLICIT, *SSL, *NONE
Data protection	*DFT	*DFT, *PRIVATE, *CLEAR
		* *
OK Cancel	Help	IEM
<	IIII	>

Appendix E: Batch FTP *Secure command parameters

The parameters in *red* are associated with the ***Secure** option.

Port

Specifies the port number used for connecting to the FTP server. If a specific port is required then supply it here. If using *DFT – it will use port 21. If *SECURE is used – The value 00990 is used. Port 990 is reserved for secure FTP servers, which use

TLS or Transport Layer Security or SSL (Secure Sockets Layer SSL).

If a Port_Value is supplied - this will be used.

Secure Connection

Specifies the type of security mechanism to be used for protecting information transferred on the FTP control connection (which includes the password used to authenticate the session with the FTP server). Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are compatible protocols that use encryption to protect data from being viewed during transmission and verify that data loss or corruption does not occur.

*DFT: If the PORT parameter specifies *SECURE or 990, *IMPLICIT is used; otherwise, *NONE is used.

*IMPLICIT: The FTP client immediately attempts to use TLS/SSL when connecting to the specified FTP server (without sending an AUTH subcommand to the server). If the server does not support implicit TLS/SSL on the specified port, or the TLS/SSL negotiation fails for any reason, the connection is closed.

*SSL: After connecting to the specified FTP server, the FTP client sends an AUTH (authorization) subcommand requesting a TLS/SSL protected session. If the server supports TLS/SSL, a TLS/SSL negotiation performed. If the server does not support TLS/SSL or the TLS/SSL negotiation fails, the connection is closed.

Data Protection

Specifies the type of data protection to be used for information transferred on the FTP data connection. This connection is used to transfer file data and directory listings. The FTP protocol does not allow protection of the data connection if the control connection is not protected. Note: The DTAPROT parameter controls the use of the PROT (protection) FTP server subcommand. The FTP client subcommand SECDATA can be used to change protection for specific FTP data connections during an FTP client session.

*DFT: If the SECCNN parameter specifies a protected control connection, *PRIVATE is used; otherwise, *CLEAR is used.

*PRIVATE: Information sent on the FTP data connection is encrypted. Note: If the SECCNN parameter specifies that the FTP control connection is not encrypted, *PRIVATE cannot be specified.

*CLEAR: Information sent on the FTP data connection is not encrypted.

Appendix F: Restart the security definition process

Important: If you must restart your security definition, this process will totally remove existing security without recourse.

- The DCM files can be deleted to restart the definition process.
- The Certificate Authority, server and user certificates, and related information are stored in different directories on the AS/400 system. DCM provides a default store location.

Certificate Authority store location

DCM uses a fixed store location for the local CA. You cannot change the location. After you create a local CA you will see the following files in a specific directory. These directories must be protected from unauthorized access. The directory and files for the CA objects are:

/QIBM/UserData/ICSS/Cert/CertAuth

Directory	
CA.TXT	CA certificate and public key
DEFAULT.KDB	CA certificate and CA private key
DEFAULT.POL	CA policy file
DEFAULT.STH	Stashed password for accessing the local CA KDB.

/QIBM/UserData/ICSS/Cert/Download/CertAuth

Directory containing the CA certificate available for distribution to clients CA.CACRT CA certificate in binary format

System certificate store location

You can select two types of locations to store a certificate. OS/400 server applications, such as HTTP and Telnet, can only use certificates stored in the ***SYSTEM** certificate store. Another selection is **OTHER**, which enables you to store certificates in any directory on the AS/400 Integrated File System (IFS).

The directory and file structure is as follows:

```
*SYSTEM (default store location)
```

/QIBM/UserData/ICSS/Cert/Server

```
Directory
```

DEFAULT.KDB System certificate(s), private key(s) and CA certificates DEFAULT.RDB Certificate request DEFAULT.STH Stashed password for automatic access to a KDB file by the server