Implementing Secure Sockets Layer (SSL) on i

Presented by Barbara Brown
Alliance Systems & Programming, Inc.
Agenda

• SSL Concepts
• History of SSL
• Digital Certificate Manager
  – Local Certificate Authority
  – Server Certificates
  – User Certificates
  – Signing Certificates
• Applications supporting SSL
• Tips on using SSL
  – Browsers
  – Firewalls
SSL Concepts

Benefits of SSL:

- Encryption (prevents data from being read in transit)
- Ensure Data Integrity (data not modified in transit)
- Authenticate Server identity
- Authenticate Client identity (SSL V3 & TLS V1)

If that isn’t enough incentive...

State Security Breach Notification Laws:

- As of December 16, 2008 Forty-four states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.
- Includes Illinois, but not Missouri, YET.
History of Secure Sockets Layer

- 1994 - SSL Version 1.0 developed by Netscape and RSA
- 1995 - Netscape and RSA create V2.0 and implement it in their products
- V2.0 has some security weaknesses and missing functionality, such as client authentication.
- 1996 - Netscape published SSL V3.0.
- V3.0 not tight enough for today’s Internet and missing functionality, such as VPN and error notification
- 1999 - Transport Layer Security Protocol V1.0 (TLS) defined by Internet Engineering Task Force (IETF)
SSL Concepts: Enhancements in TLS

- **Can be used to tunnel an entire network stack to create a Virtual Private Network (VPN)**
- **Key-Hashing for Message Authentication**
  - Key-Hashing for Message Authentication Code (HMAC) ensures that record cannot be altered while traveling over an open network such as the Internet.
  - More secure than Message Authentication Code (MAC) used by SSL Version 3.0
- **Enhanced Pseudorandom Function (PRF)**
  - Two hash algorithms used to generate key.
- **Improved finished message verification**
  - Both TLS Version 1.0 and SSL Version 3.0 provide finished message to both endpoints to authenticate that exchanged messages not altered.
  - TLS bases this finished message on the PRF and HMAC values, which is more secure than SSL Version 3.0.
- **Consistent certificate handling**
  Unlike SSL Version 3.0, TLS attempts to specify the type of certificate which must be exchanged between TLS implementations.
- **Specific alert messages**
  - More specific alerts for more types of problems detected by either endpoint.
  - Documents when certain alerts should be sent.
SSL Concepts

- **Handshake protocol**
  - authenticates one or both endpoints of the SSL session
  - establishes a unique symmetric key used to generate keys to encrypt and decrypt data for that SSL session.

- **Record protocol**
  - controls the flow of the data between the two endpoints of an SSL session.

- **Digital certificate**
  - issued by a Certificate Authority
  - can be assigned to endpoints or to applications using SSL on each endpoint of the connection.
  - comprised of a public key and some identifying information that a trusted Certificate Authority (CA) has digitally signed.
  - Each public key has an associated private key stored separately from certificate.
SSL Concepts

Data encryption and decryption:
- Server sends its certificate to client
- Optionally, server may request client certificate (SSL V3)
- Client creates secret key, encrypts it with server’s public key, and sends encrypted key back.
- Server uses its private key to decrypt the secret key
- From then on, secret key is used (requires less computation than public/private key pairs)
- Secret key automatically expires after a specific time. (24 hours recommended for V3.0)
SSL Concepts: Handshake

1.) Request secure connection

2.) Send server's certificate to client

3.) Check it to use the certificate

4.) Send available ciphers to the server

5.) Send chosen cipher to the client

6.) Create a secret key and encrypt it using the server's public key

7.) Send the encrypted secret key to the server

8.) Decrypt the secret key using server's private key

Handshake end

At least 2 Certificates required: Server Certificate and Issuer’s (CA) Certificate
SSL History on i

- **SSL Introduced with OS/400 V4R1**
  - Limited support (HTTPS – no telnet, FTP, client certificates...)
- **Added applications and enhanced support over time**
- **V5R4** –
  - **Cryptographic Access Provider product** functionality integrated in OS
- **V6R1** –
  - **System SSL**
    - generic services provided in i5/OS® Licensed Internal Code (LIC)
    - tightly coupled with operating system and sockets code
    - extra performance and security.
    - APIs
  - **New System Values**
    - QSSLPCL – SSL protocols
    - QSSLCSLCTL – system or user control of cipher list
    - QSSLCSL – cipher specification list

March 12, 2009
Current State of SSL Support on i

- Enterprise Identity Mapping (EIM)
- FTP server
- IBM® HTTP Server for i5/OS®
- System i Access for Windows®
- IBM Tivoli® Directory Server for i5/OS
- Distributed relational database architecture (DRDA®) and distributed data management (DDM) server
- Management Central
- Telnet server
- Websphere Application Server — Express
- Applications written to the System i Access for Windows set of APIs
- Applications developed using Global Secure Toolkit (GSKit) and SSL System i APIs.
iSeries Requirements for SSL

- **Digital Certificate Manager**
  - (DCM) (5761-SS1 Option 34)
  - Note: IBM Java™ Secure Socket Extension (JSSE) and OpenSSL do not require DCM.

- **TCP/IP Connectivity Utilities for i5/OS®**
  - (5761-TC1)

- **HTTP Server for i5/OS**
  - (5761-DG1)

- **IBM Developer Kit for Java**
  - (5761–JV1)
  - required to start HTTP admin server

- Cryptographic hardware can be used with SSL to speed up SSL handshake processing
  - requires Cryptographic Service Provider.

- **Client must also support SSL**
SSL Concepts: Certificate Authority

- Organization that issues digital certificate
- Should have controls to prevent fraud
- Internet Certificate Authorities
  - National Certificate Authorities: Certiposte, Asociación Nacional de Notariado Mexicano, Deutsche Telekom, Belgacom
  - GTE Cybertrust
  - Integrion
  - RSA
  - Thawte
  - VeriSign
    - and more...
- Can be your own certificate authority
SSL Concepts: Which Certificate Authority?

Use an Internet Certificate Authority when...
- You are serving SSL across the Internet
- You are serving SSL to the general public, customers, or business partners that require the assurance of a third party CA
- You are serving SSL to an intranet and do not want to have to train users how to receive your CA certificate into their browsers.
- You do not want to operate your own CA.
- You want to accept certificates that users already have.
- The number of certificates to be issued is large and you do not want the job of having to validate the information people give.

Be your own certificate authority when...
- You want to operate your own CA to control the issuing process.
- You want to identify users in advance.
- Trust is based on organization.
Create a Certificate Authority

http://your400:2001

IBM HTTP Server for iSeries
Configure the iSeries HTTP Server and SSL

Digital Certificate Manager
Create, distribute, and manage Digital Certificates

IBM IPP Server for iSeries
Configure the IBM IPP Server

Related task information

March 12, 2009
Create a Certificate Authority

Each certificate store has its own password. REMEMBER YOUR PASSWORD!!

Alas… all certificates expire… NOTE IT ON YOUR CALENDAR a month in advance!
Create a Certificate Authority

March 12, 2009

Do receive the certificate and save it on a server somewhere and in your own file system: When using Local CA, you need to import Local CA certificate to the other systems certificate store and set it as trusted.
Create a Certificate Authority

Think about how long you want the certificates you issue to last.

March 12, 2009
Create a Certificate Authority

Only applications enabled for SSL will show up in this list...
If you have not yet enabled SSL for your HTTP or Websphere application server you won’t see it here and will have to return later to do this.
Create a Certificate Authority

System Server Certificate used by SSL enabled Server applications
Server Certificate

- Digital ID
- Issued by Certifying Authority
- Standardized format (X.509 - RFC 2459)
- private key of the certificate’s public key is held by the entity to whom the certificate was issued and sometimes other trusted parties
- A certificate typically holds:
  - serial number.
  - name of the entity it was created for
  - public key of the certificate.
  - period for which the certificate is valid.
  - name of the CA that issued the certificate
  - digital signature from the CA that issued the certificate. (used to prove the validity of the certificate)
Create Server Certificate

Another password to remember.
Create Server Certificate

Only applications enabled for SSL will show up in this list...
If you have not yet enabled SSL for your HTTP or Websphere application server you won’t see it here and will have to return later to do this.
Create Server Certificate

You can only create certificates if you are acting as your own Certificate Authority. If you are NOT acting as your own Certificate Authority, you will need to Request a Certificate.
You must select the System certificate Store to work with certificates for your system, then enter the password on the next screen.
Create a Certificate Request
Create a Certificate Request

Digital Certificate Manager

Select a Certificate Authority

Certificate Authority that will sign this certificate:

- Local Certificate Authority
- VeriSign or other Internet Certificate Authority

March 12, 2009

Alliance
Systems & Programming
Create a Certificate Request

Digital Certificate Manager

Create a System Certificate

The system will create a public-private key pair and store the key pair in the certificate store listed below.

Certificate store: *SYSTEM

Key size: 2048 (bits)

Key label: VeriSignServerCertificateTrial (required)

Certificate Information

Server name: www.yourservice.com (required)

Organization unit: ITSO Raleigh

Organization name: IBM

Locality or city: Cary

State or province: North Carolina (required)

Country: US (required)

Zip or postal code: 

[OK] [Cancel]
Create a Certificate Request

Select the ENTIRE certificate request, beginning with

-----BEGIN NEW CERTIFICATE REQUEST-----

and ending with

-----END NEW CERTIFICATE REQUEST-----

And COPY it (Ctl C)
Create a Certificate Request

Then PASTE it into your certificate request submission to your chosen Certifying Authority.
Receive Certificate from Issuer

Select the ENTIRE certificate, beginning with
-----BEGIN CERTIFICATE-----
and ending with
-----END CERTIFICATE-----
And COPY it, then paste it into an editor like Notepad and save it to a text file on the IFS
(you will also want to save a copy in another secure location)

March 12, 2009

Alliance Systems & Programming
Receive Certificate from Issuer

Import the file you saved on the IFS
Receive Certificate from Issuer

Next you need to identify the applications that will use the certificate
Work with Certificates

- **Renew Certificate**
  - make sure you have a reminder on your calendar!

- **Validate Certificate**
  - certificate is not expired
  - not listed in a Certificate Revocation List (CRL) as revoked
  - CA certificate for the issuing CA in the current certificate store
  - CA certificate is enabled and marked as trusted

- **Import Certificate**
  - from another 400 or from Internet CA

- **Export Certificate**
  - Only for another 400 (Bummer!)
  - Windows Server has Certificate Authority for working with certificates in Windows environment
**View Certificate**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name</td>
<td><a href="http://www.yourservers.com">www.yourservers.com</a></td>
</tr>
<tr>
<td>Organization unit</td>
<td>ITSO Raleigh</td>
</tr>
<tr>
<td>Organization name</td>
<td>IBM</td>
</tr>
<tr>
<td>Locality or city</td>
<td>Cary</td>
</tr>
<tr>
<td>State or province</td>
<td>North Carolina</td>
</tr>
<tr>
<td>Zip or postal code</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name</td>
<td>For VeriSign authorized testing only. No assurances</td>
</tr>
<tr>
<td>Organization name</td>
<td>VeriSign, Inc</td>
</tr>
<tr>
<td>Locality or city</td>
<td></td>
</tr>
<tr>
<td>State or province</td>
<td></td>
</tr>
<tr>
<td>Zip or postal code</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td></td>
</tr>
</tbody>
</table>

Associated key label: VeriSignServerCertificate Thiên

<table>
<thead>
<tr>
<th>Key length</th>
<th>2048</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private key</td>
<td>Yes</td>
</tr>
<tr>
<td>Trusted</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Renew Certificate

Digital Certificate Manager

Renew Certificate

Certificate type: Server or client
Certificate store: *SYSTEM
Default certificate label: Alliance website

Select a certificate, then select a button to perform an action on the certificate.

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Common name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alliance website</td>
<td>ASPWEB.ALLIANCESYS.COM</td>
</tr>
<tr>
<td>Alliance ASPWEB</td>
<td>ASPWEB.ALLIANCESYS.COM</td>
</tr>
</tbody>
</table>

March 12, 2009

March 12, 2009
Renew Certificate

Digital Certificate Manager

Select a Certificate Authority (CA)

Certificate type: Server or client
Certificate store: *SYSTEM
Certificate label: Alliance ASPWEB

Select the type of Certificate Authority (CA) that will sign this certificate.

- Local Certificate Authority (CA)
- VeriSign or other Internet Certificate Authority (CA)

Continue | Cancel

March 12, 2009

Alliance Systems & Programming
Renew Certificate

Digital Certificate Manager

Renew Certificate
Certificate type: Server or client
Certificate store: *SYSTEM
Original certificate label: Alliance ASPWEB

Use this form to renew the certificate. Please provide any missing information.

New certificate label: (required)
Key size: 1024 (bits)

Certificate Information
Common name: ASPWEB.ALLIANCESYS.COM (required)
Organization unit:
Organization name: Alliance Systems & Programming (required)
Locality or city:
State or province: Missouri (required, minimum of 3 characters)
Country or region: US (required)

Subject Alternative Name
Note: Certificate extensions are not necessary for Secure Sockets Layer (SSL), but are recommended for Virtual Private Network (VPN).
IP version 4 address:
Fully qualified domain name:
(host_name domain_name)
E-mail address:
(user_name@domain_name)

March 12, 2009

Certificate Label must be Unique – I have started putting the expiration date in it

This screen for LOCAL Certificate Authority renewal only
Renew Certificate

Digital Certificate Manager

Renew Certificate

Certificate type: Server or client
Certificate store: *SYSTEM
Certificate label: Alliance ASPWEB

Create a new public-private key pair for this certificate?

☐ Yes - Create a new key pair for this certificate.
☒ No - Import the renewed signed certificate from an existing file.

Yes – creates a new request
No – import a new certificate from the CA

Continue  Cancel

March 12, 2009
Renew Certificate

Certificate Renewed Successfully

Message: Your certificate was renewed and placed in the certificate store listed below:

Certificate type: Server or client
Certificate store: *SYSTEM
Certificate label: ASPWEB.ALLIANCESYS.COM, exp 9-2005

Select which applications will use this certificate:

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.

Select All  Clear All

<table>
<thead>
<tr>
<th>Application</th>
<th>Type</th>
<th>Assigned certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS/400 TCP Central Server</td>
<td>Server</td>
<td>Alliance website</td>
</tr>
<tr>
<td>OS/400 TCP Database Server</td>
<td>Server</td>
<td>Alliance website</td>
</tr>
<tr>
<td>OS/400 TCP Data Queue Server</td>
<td>Server</td>
<td>Alliance website</td>
</tr>
<tr>
<td>OS/400 TCP Network Print Server</td>
<td>Server</td>
<td>Alliance website</td>
</tr>
<tr>
<td>OS/400 TCP Remote Command Server</td>
<td>Server</td>
<td>Alliance website</td>
</tr>
<tr>
<td>OS/400 TCP Signon Server</td>
<td>Server</td>
<td>Alliance website</td>
</tr>
<tr>
<td>Directory Services server</td>
<td>Server</td>
<td>Alliance website</td>
</tr>
<tr>
<td>Directory Services publishing</td>
<td>Client</td>
<td>Alliance ASPWEB</td>
</tr>
</tbody>
</table>
Manage Applications

- **Update Certificate Assignment**
  - Make sure all your applications that will use SSL have a valid certificate assigned!

- **Validate Application**
  - certificate is assigned for the application
  - ensures that assigned certificate is valid
  - if the application is configured to use a Certificate Authority (CA) trust list, that trust list contains at least one CA certificate
  - CA certificates in the application CA trust list are valid

- **View Application Definition and Add Application**
  - Can define your OWN applications & configure SSL
Define CA trust list

Digital Certificate Manager

Define CA Trust List

Application type: Server
Application ID: QIBM_GL_DIRSVR_SERVER
Application description: Directory Services server

Must define trusted CAs for EACH APPLICATION

Remember: application must be enabled for SSL before it will show up in the list!

Note: The Certificate Authorities (CAs) defined in the CA trust list for the application are checked. If you wish to change the trust list, click on the check box and select OK.
Certificate Revocation List Location

Digital Certificate Manager

Add CRL Location

The Certificate Revocation List (CRL) location is the LDAP server where the CRL is stored. Use this form to define the location of the CRL.

CRL Location Name

LDAP Server Information:

- LDAP Server: 
- Use Secure Sockets Layer (SSL): Yes
- Port number: 

Connection Information:

- Login distinguished name (DN): 
- Password: 

Note: To use an anonymous session, leave the login distinguished name (DN) and password blank.

OK  Cancel

LDAP server can provide a list of revoked certificates
Public Key Infrastructure (PKIX) Request Location

- PKIX Certificate Authorities require proof of identity from certificate requester through a Registration Authority (RA) before issuing certificate
- Configure a URL for a PKIX CA
- DCM provides PKIX CA as option for obtaining signed certificates
- Lotus(R) Domino(TM) provides a PKIX CA for public use
Enable SSL for HTTP Admin Server

1) Make sure that the ADMIN server is running.
2) Click the Manage tab …then Click the All HTTP Servers subtab.
3) Select ADMIN from the Server list.
4) Select Include /QIBM/UserData/HTTPA/admin/conf/admin-cust.conf from the Server area list.
5) Expand Tools and Select Edit Configuration File.
6) Enter the following information into the configuration file or remove the "#" symbol to uncomment these lines:

   LoadModule ibm_ssl_module /QSYS.LIB/QHTTPSVR.LIB/QZSRVSSL.SRVPGM
   Listen 2001
   Listen 2010
   SetEnv HTTPS_PORT 2010
   <VirtualHost *:2010>
     SSLEnable
     SSLAppName QIBM_HTTP_SERVER_ADMIN
   </VirtualHost>

7) Click OK.
Enable SSL for HTTP Admin Server

# Customer additions to the admin configuration
LoadModule ibm_ssl_module /QSYS.LIB/QHTTPSVR.LIB/QZSRVSSL.SRVPGM
Listen 2001
Listen 2010
SetEnv HTTPS_PORT 2010
<VirtualHost *:2010>
  SSLEnable
  SSLAppName QIBM_HTTP_SERVER_ADMIN
</VirtualHost>
Enable SSL for HTTP Admin Server

(continued)

8) Go to the Digital Certificate Manager.
9) Click Select a Certificate Store.
10) Select *SYSTEM, then enter a password in the Certificate store password field on the next screen.
11) Expand Manage Applications and Select Update certificate assignment.
12) On the application type screen, select Server.
13) Select QIBM_HTTP_SERVER_ADMIN application name. (If it doesn’t show up in the list, you may need to manually ADD the Application to the list using the parameters shown here, then come back to step 11 Update Certificate Assignment... If you END and restart the admin server to make it show up,...

GOTCHA!!! the admin server will fail to start because it doesn’t have a certificate assigned!!

Catch-22!)

If you’re stuck with an admin config file that won’t start, you can get to it on a green screen with the command
WRKLNK ‘/qibm/userdata/httpa/admin/conf’
Use option 2 to edit admin-cust.conf and put a # in the first position of the SSLENABLE and SSLAPPNAME lines to comment them out. Then save the file and STRTCPSVR *HTTP_HTTPSVR(*ADMIN)

March 12, 2009
Enable SSL for HTTP Admin Server (continued)

14) Click **Update Certificate Assignment**.
15) Select the appropriate certificate.
16) Click **Assign New Certificate** to assign the certificate to the application name selected in the previous step.
17) If you had to manually add the application, next select **Define CA Trust List**, select **Server**, then select the server application you added (**QIBM_HTTP_SERVER_ADMIN**) and click **DEFINE CA TRUST LIST**. On the next screen click the **Trust All** button, then click **OK**.
18) Restart the ADMIN server
   - **ENDTCPSVR *HTTP HTTPSVR(*ADMIN)**
   - **STRTCPSVR *HTTP HTTPSVR(*ADMIN)**
19) Restart your Web browser.

To use the ADMIN server, type `http://[iSeries_hostname]:2001` for a non-secure connection or `https://[iSeries_hostname]:2010` for a secure connection.

**Note:** If you have trouble getting the secure connection working, check the ADMIN error log file located in the (`\QIBM\UserData\HTTPA\admin\logs\` directory for information.
iSeries Server Applications that Support SSL

- iSeries Access
  - dataqueue
  - database
  - file server
  - network printer
  - Remote command
  - management central
  - signon
- DRDA & DDM (database access)
- FTP (file transfer)
- Telnet (terminal access)
- HTTP (original & Apache)
- Host on Demand
- Host Access Transform Server (HATS) & HATSLE

- Websphere Application Server
- Domino
- LDAP (directory services)
- EIM (Enterprise Identity Mapping)
- Applications written with:
  - Java Developer Kit or IBM Toolbox for Java
  - iSeries Access for Windows APIs
  - Global Secure Toolkit (GSKit)
  - SSL_iSeries Native APIs
Applications that support SSL: iSeries Access

1) Authorize the appropriate user profile to the Client Encryption products.
   WRKAUT OBJ('/QIBM/ProdData/CA400/EXPRESS/SSL/SSL40')
   or... use iSeries Navigator to edit permissions of SSLxx under Integrated File System

2) Install the SSL component of iSeries Access
   - Use Selective Setup…
Applications that support SSL: iSeries Access (continued)

- IBM Key Management Utility
  – Comes with iSeries
Applications that support SSL: iSeries Access (continued)

3) Add CA Cert using IBM Key Management Utility
   - Open iSeries Access key database file: cwbssldf.kdb
Applications that support SSL: iSeries Access

3) Use Download utility to add CA cert to iSeries Access key database

4) Activate SSL for the iSeries Navigator client:
   
   – In iSeries Navigator, expand My Connections.
   – Right-click the system, and select Properties.
   – Click the Secure Sockets tab and select Use Secure Sockets Layer (SSL) for connection.
   – Exit iSeries Navigator and restart it.
Applications that support SSL: Original IBM HTTP server

1. Enable SSL in the HTTP server configuration

2. Assign the CA and Server certificate to the web server instance
Applications that support SSL:
Apache HTTP Server

1) Set up a name-based virtual host
   - Click the Manage tab, then Click the HTTP Servers subtab.
   - Select your HTTP Server (powered by Apache) from the Server list.
   - Select Global configuration from the Server area list.
   - Expand Server Properties and Click Virtual Hosts, then Click the Name-based tab in the form.
   - Click Add under the Named virtual hosts table.
   - Enter an IP address in the IP address column and a port number in the Port column. Example: 443
   - Specify a port number to be used for SSL – default is 443
   - Click Add under the Virtual host containers table in the Named host column. Note: This is a table within the Named virtual hosts table in the Named host column.
   - Enter the fully qualified server hostname for the virtual host in the Server name column.
   - Note: Make sure the server hostname you enter is fully qualified and associated with the IP address you selected in the iSeries TCP/IP host table
   - Enter a document root for the virtual host index file or welcome file in the Document root column.
   - Click Continue, then Click OK
Applications that support SSL: Apache HTTP Server (continued)

2) Set up Listen directive for virtual host
   - Expand **Server Properties**, Click **General Server Configuration**, then Click the **General Settings** tab
   - Click **Add** under the **Server IP addresses and ports to listen on table**.
   - Select the IP address you entered for the virtual host in the **IP address** column.
   - Enter the port number you entered for the virtual host in the **Port** column.
   - Click **Continue**, then Click **OK**.

3) Set up the virtual host directories
   - Select the virtual host from the **Server area** list.
   - Expand **HTTP Tasks and Wizards**, Click **Add a Directory to the Web**, then Click **Next**.
   - Select **Static web pages and files** and Click **Next**.
   - Enter a directory name for the virtual host in the **Name** field. Click **Next**.
   - Enter an alias for the virtual host in the **Alias** field. Example: /earnings/
   - Click **Next**, then Click **Finish**.
   The document root and directory for the virtual host has been created.
Applications that support SSL: Apache HTTP Server

4) Set up password protection via authentication
   - Select the directory under the virtual host from the Server area list.
   - Expand Server Properties, Click Security, then Click the Authentication tab in the form.
   - Select Use OS/400® profile of client under User authentication method for 400 native security
   - Enter iSeries Signon in the Authentication name or realm field.
   - Select Default server profile from the OS/400 user profile to process requests list under Related information. When selected, the value %%SERVER%% will be placed in the field.
   - Click Apply, then Click the Control Access tab in the form.
   - Click All authenticated users (valid user name and password) under Control access based on who is making the request, then Click OK.

5) Enable SSL for the virtual host
   - Select the virtual host from the Sever area list. Example: Virtual Host *:443
   - Expand Server Properties, then Click Security.
   - Click the SSL with Certificate Authentication tab in the form.
   - Select Enable SSL under SSL.
   - Select QIBM_HTTP_SERVER_[server_name] from the Server certificate application name list. Note: Remember the name of the server. You will need to select it again in the Digital Certificate Manager.
   - Select Do not request client certificate for connection under Client certificates when establishing the connection then Click OK.
Applications that support SSL: Apache HTTP Server

6) Associate system certificate with HTTP Server (powered by Apache)
   - Go to Digital Certificate Manager (http://yourserver:2001)
   - Click Select a Certificate Store, Select *SYSTEM, then Click Continue.
   - Enter a password in the Certificate store password field and Click Continue.
   - Click Manage Applications, Select Update certificate assignment, then Click Continue.
   - Select Server and Click Continue.
   - Select the appropriate application name and Click Update Certificate Assignment.
   - Select the appropriate certificate.
   - Click Assign New Certificate. This assigns the certificate to the application name selected in the previous step.

7) Restart your HTTP Server (powered by Apache)
   - Go to HTTP Administration and Click the Manage tab.
   - Click the HTTP Servers subtab.
   - Select your HTTP Server from the Server list.
   - Click the Stop icon if the server is running.
   - Click the Start icon.

8) Test your HTTP Server (powered by Apache)
   - Start a new Web browser.
   - Enter https://yourserver:port in the location or URL field.
Applications that support SSL: FTP

- **Enable SSL for the iSeries FTP server by:**
  - In iSeries Navigator, expand the iSeries server --> Network --> Servers --> TCP/IP.
  - Right-click FTP.
  - Select Properties, then Select the General tab.
  - Choose Secure only for SSL support
  Select this to allow only SSL sessions with the FTP server. Connections may be made to the non-secure FTP port, but the FTP client must negotiate an SSL session before the user is allowed to log in.

- **Enable SSL for the iSeries FTP Client Control Connection by:**
  - On the STRTCPFTP (FTP) command, specify SECCNN (*SSL)
  - Within your FTP client session, use the SECOPEN subcommand

- **Enable SSL for the iSeries FTP Data Connection**
  - For the STRTCPFTP (FTP) command, enter DTAPROT (*PRIVATE)
  - When you have a secure control connection, you can use the SECDATA subcommand to change the data connection protection level.
Applications that support SSL: Telnet Server

- **Remove any port restrictions**
  - Using iSeries Navigator, expand iSeries server --> Network.
  - Right-click TCP/IP Configuration and select Properties.
  - Click the Port Restrictions tab to see a list of port restriction settings.
  - Select the port restriction that you want to remove and click Remove, then click OK.

- **Enable SSL for Telnet**
  - Expand *My iSeries server* --> Network --> Servers --> TCP/IP.
  - Right-click *Telnet*, Select *Properties*, Select the *General* tab.
  - Choose one of these options for SSL support:
    - **Secure only**
      Select this to allow only SSL sessions with the Telnet server.
    - **Non-secure only**
      Select this to prohibit secure sessions with the Telnet server. Attempts to connect to an SSL port will not connect.
    - **Both secure and non-secure**
      Allows both secure and non-secure sessions with the Telnet server.

- **Configure the Telnet server to require certificates for client authentication**
  by selecting YES to require client authentication on DCM Application Definition for Telnet server application.
Applications that support SSL: Telnet Client (continued)

• **Enable iSeries Access Client for SSL**
  – Open iSeries Navigator.
  – Right-click the name of your system, Select **Properties**.
  – Select the **Secure Sockets** tab. **Note:** This tab will not appear unless you have completed a selective install of iSeries Client Encryption (128-bit), 5722-CE3.
  – Click **Download** to download the CA certificate into the key database.
  – Enter your key database password (default is ca400)

• **Configure telnet session to use SSL and port 992**

This is all that is required to encrypt the session and validate the server certificate. If you want to also validate the user, you must use User Certificates
User Certificates

- Used to authenticate user to a particular server
  - additional security
  - replace userid and password security
  - digital signature

NOTE: The only way to create client user certificates using the AS/400 DCM is for the user to come to the DCM using a browser. The user has to enter the AS/400 system user name and password, and then request a certificate. The user profile must exist in advance. There is no way to create a certificate on behalf of another entity, nor to modify the creation of the certificate by using an exit program or something similar. When the certificate has been created, it is automatically associated with the user name that was given.
Applications that support SSL: Telnet Client

User Certificates

• **Obtain a user certificate**
  - Start DCM (http://yourserver:2001)
  - In the left-hand navigation frame, select **Create Certificate** to display a list of tasks.
  - From the task list, select **User Certificate** and click **Continue**.
  - Complete the **User Certificate** form. Only those fields marked "Required" need to be completed. Click **Continue**.
  - Depending on the browser you use, you will be asked to generate a certificate that will be loaded into your browser. Follow the directions provided by the browser.
  - When the **Create User Certificate** page reloads, click **Install Certificate**. This will install the certificate in the browser.
  - Export the certificate to your PC. You must store the certificate in a password-protected file.

• **Enable iSeries Access to present certificate**
  - Start the **IBM Key Management Utility**
  - You will be prompted for your key database password. Unless you have previously changed the password from the default, enter ca400. A confirmation message displays. Click **OK**.
  - From the pull-down menu, select **Personal certificates**.
  - Click **Import**.
  - In the **Import key** display, enter the file name and path for the certificate. Click **OK**.
  - Enter the password for the protected file. This is the same password that you specified when you create a user certificate in DCM. Click **OK**. When the certificate has been successfully added to your personal certificates in IBM Key Management, you can use PC5250 emulator or any other Telnet application.
Signing Certificates

• Digitally sign objects to verify
  – Integrity of the object's contents
  – Object’s source of origin

• Use DCM to:
  – Issue signing certificates
  – Sign Objects
    • Can also use Management Central as of V5R2
  – Verify signatures on objects
Working with Certificates in Browsers

Adding certificate authority to browser prompted when new certifying authority or server certificate received

Internet Explorer: tools...internet options...content

Netscape Navigator:

Communicator...tools...security info

You can double click on the lock in the lower right-hand corner of a secured page in IE to view the certificate!
Importing a Certificate to Internet Explorer

1) Access the Certificate Import wizard from the view certificate window.

2) Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site’s security certificate.
   - The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
   - The security certificate has expired or is not yet valid.
   - The name on the security certificate is invalid or does not match the name of the site.
   Do you want to proceed?
   - Yes
   - No
   - View Certificate

3) 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:
     - Automatically select the certificate store based on the type of certificate
     - Place all certificates in the following store:

4) Completing the Certificate Import Wizard
   - You have successfully completed the Certificate Import wizard.
   - You have specified the following settings:
     - Certificate Store Selected: Automatically determined by
       - Content
       - Certificate

5) The import was successful.
Exporting Certificate with Internet Explorer

1) Access the Certificate Export wizard from Tools... Internet Options...Content... Certificates

2) Select the format you want to use:
   - DER encoded binary X.509 (.CER)
   - Base64 encoded X.509 (.CER)
   - Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
   - Include all certificates in the certification path if possible
   - Enable strong protections (requires IE 5.5, NT 4.0 SP3 or above)

3) Specify the name of the file you want to export
   - File name: C:\BA\trust\certifikate.cer

4) Completing the Certificate Export Wizard
   - You have successfully completed the Certificate Export wizard
   - You have specified the following settings:
     - File Name: C:\BA
     - Include all certificates in the certification path: No
     - File Format: DER

5) The export was successful.

March 12, 2009
Certificate Support in Firefox

• Less restrictive errors
• Easier ‘import’ certificate permanently
Using SSL with Firewalls

Firewalls considerations: what ports needed?
- Secure HTTP (https:) - port 443
- Secure FTP – 990
- Secure Telnet - port 992
- Secure DDM/DRDA - port 448
- Secure iseries access ports:
  - Management Central – 5566
  - Central server - 9470
  - Database server - 9471
  - Data Queue - 9472
  - File Server - 9473
  - Network Print - 9474
  - Remote Command - 9475
  - Signon Server – 9476

AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659-00)
Implementing Secure Sockets Layer (SSL) on I

THANK YOU

Presented by Barbara Brown
Alliance Systems & Programming, Inc.
bbrown@alliancesys.com