Using SSL with Client Access Express for AS/400

The AS/400 Operating System, OS/400, supports Secure Socket Layer (SSL) since its release of V4R1. It is not until V4R4 and the release of Client Access Express that communication between Client Access for Windows and the AS/400 is secure.

Companies that have the Client Access as their communication application with the AS/400, now have the important task of securing these links. As well as those who are planning to use Client Access for this purpose.

This paper is meant to help those who are in need of securing a Client Access connection with their AS/400. We will achieve this security with the use of SSL on the link. SSL support on the AS/400 can be used with different applications and in different forms, but this paper will refer only to Client Access for Windows.

Digital Certificates

Digital Certificates are a form of identification that can be verified electronically. They can be used not only for individuals, but any entity such as a computer. Certificate Authorities (CA) are responsible for issuing digital certificates. CAs are entities entrusted to issue digital certificates and prevent fraud. The AS/400 Digital Certificate Manager (DCM) application can serve as a CA.

Digital Certificates are used as the basis of communications for the SSL protocol. To establish an SSL session, only the server is required to have a digital certificate. SSL is commonly used by Hypertext Transfer Protocol (HTTP) applications, where the client browser doesn't necessarily own a digital certificate. The client browser has to trust the CA that issued the HTTP server's digital certificate.

The specific steps required to create a digital certificate varies according to the CA responsible for the creation. Some general steps are as follows:

- The client expresses the wish to create a digital certificate to a specific CA.
- There will have to be some form that the client needs to fill out, for the CA to gather information. The specific information on the form varies from one CA to another.
- When the client submits the form with the required information, he will be requested to create a private key.
- At this point, the client receives instructions on how to obtain the digital certificate from the CA.
- After the CA completes validation of the client, the client receives the digital certificate and it can be used immediately.

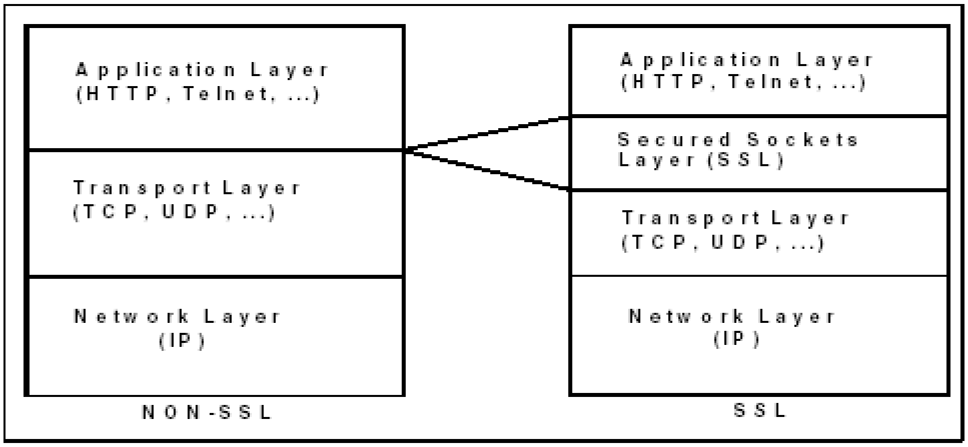
Some CA allows additional information to be placed in their digital certificates. This optional information can be used with specific applications and in special situations. However, the AS/400 DCM does not allow for additional information in its digital certificates.

You have the alternative to choose the AS/400 DCM to be your CA, or choose one of the well-known CA on the Internet. When you pick a well-known CA, you don't have to download a CA certificate and install it on the client. You would need to do this to have the client trust the CA, but a well-known CA is trusted automatically. On the other hand, you need to pay a license to the well-known CA to issue your AS/400 system certificate and of course you lose control over them as well.

For control of our servers' certificates, to avoid involving another entity in the process and to minimize cost for implementing SSL on Client Access Express applications, it has been chosen to use the AS/400 DCM as the CA. Keep in mind that if you have other applications running on your AS/400 that need the use of SSL communications, you might want to use a well-known CA, depending on your existing infrastructure. In this paper, it is assumed that SSL has not been used on any of the AS/400 applications.

SSL Overview

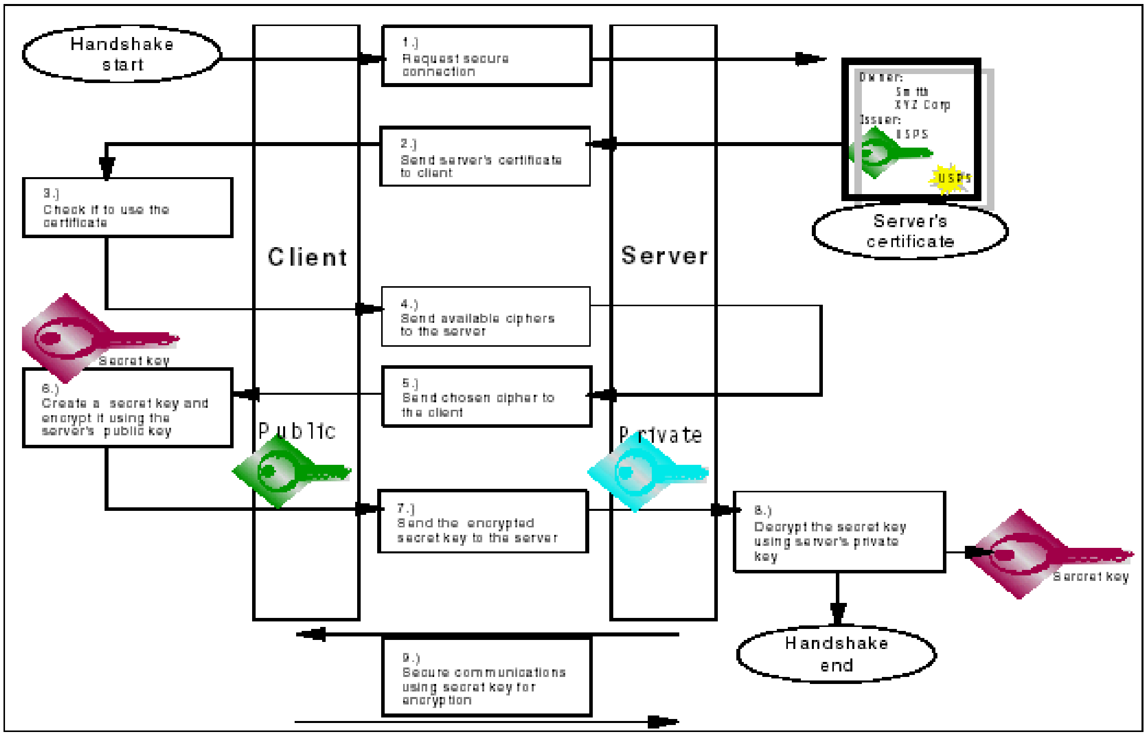
The SSL protocol provides end-to-end encryption between a client and a server. This protocol works between the transport (TCP and UDP) and the application (Telnet, FTP, HTTP…) layers of the TCP/IP protocol suite, as shown in the picture below.



SSL provides confidentiality, integrity, authentication and non-repudiation. This is achieved by three different functions. The first function is data encryption and decryption. This function ensures that data being transmitted cannot be read by someone other than the intended recipient if intercepted. This function is accomplished with products 5769-AC1, 5769-AC2 or 5769-AC3 on the AS/400 (server) side and with 5769-CE1, 5769-CE2 or 5769-CE3 on the PC side (client). As you go from AC/CE1 to AC/CE2 to AC/CE3 the level of security on the link increases. Therefore, these two products, the one on the AS/400 and the one on the PC, are paired to achieve the highest level of security supported by both entities.

The second function is accomplished by the use of Message Authentication Codes (MACs), which allow any changes to the data being sent to be detected and rejected, if desired. The third main function carried on by SSL is the option of each party to identify the identity of the other. Digital certificates are used to conduct this function. Although SSL V3 supports authentication for the server and the client, the SSL communication with Client Access Express to the AS/400 allows only server authentication for all Client Access Express applications except for 5250 emulation sessions. 5250 emulations sessions, both display and printer mode, are the only Client Access Express application that accept server and client authentication via digital certificates. Although 5250 emulations are the exception, this paper will not cover client authentication for 5250 emulation sessions.

SSL actually consists of two protocols: SSL record protocol and SSL handshake protocol. The SSL record protocol is used for the encapsulation of different higher-level protocols. The SSL handshake protocol allows the client and the server to authenticate each other and to


Handshake start
1.) Request secure connection
Owner: Smith XYZ Corp
Issuer: USPS
USPS
Server's certificate
2.) Send server's certificate to client
3.) Check if to use the certificate
Client
Server
4.) Send available ciphers to the server
Secret key
6.) Create a secret key and encrypt it using the server's public key
5.) Send chosen cipher to the client
Public
Private
7.) Send the encrypted secret key to the server
8.) Decrypt the secret key using server's private key
Secret key
Handshake end
9.) Secure communications using secret key for encryption

exchange session specific information like encryption algorithms and cryptographic keys, before the higher application can start transmitting or receiving data. The picture below shows the SSL handshake with server certificate only.

The use of digital certificates on each main function of SSL will now be described. For data encryption and decryption, a secret key is generated for each session. Secret keys are used since they have better performance than public/private key encryption. In order to exchange the secret key securely between server and client, the public and private key of the server (at the minimum) are needed. First, one of the parties, usually the server, sends its certificate to the client, which contains the server's public key. At this point, the server could ask the client for its certificate (client authentication) and then the client generates the secret key and encrypts it with the server's public key, which is found in the server's certificate, and sends it to the server. The server decrypts the secret key with its private key and from there on only the secret key is used to encrypt the data being transmitted. For additional security, the secret key usually is set to expire after some specified time.

Data integrity also uses the secret key already exchanged. To assure the integrity of the data transmitted, a message digest is used. This is a hash function that is run through the original data being sent, which generates a small string of bits. The result of this hash function is in turn encrypted and sent to the other party with the original message. The receiver can take the original message received and also take the same hash function to generate the same message digest and then decrypt the message digest that was sent with the original data and look for a match between both. When a difference is encountered, the original message has been changed and should be sent again. When possible, the public and private key pair is used to encrypt and decrypt message digests because it provides better authentication than symmetric keys or secret keys.

When authenticating, each party can use a digital certificate to identify one another. The digital certificate from one party is sent to the second. This digital certificate contains the digital signature of the CA that issued it and that the second party trust, ensuring the first party's identity. Similarly, the second party is identified by the first.

Hardware/Software Requirements

On the AS/400 system to which you need to connect:

- **Operating System V4R4M0.** This requirement is for using SSL with the Client Access Express application.
- **5769-TC1: TCP/IP Connectivity Utilities for AS/400.**
- **5769-SS1 option 12: Host Servers.** This option allows PCs with Client Access to communicate with an AS/400 system, whether they are using SSL or not.
- **5769-SS1 options 34: Digital Certificate Manager.** You need Digital Certificate Manager to create your Certificate Authority and maintain your Digital Certificates.
- **5769-DG1: IBM HTTP Server for AS/400.** This product is required to access DCM browser-based interface.
- **5769-ACx: Cryptographic Access Provider.** The "x" value determines the maximum key length allowed for cryptographic algorithms. They are also used to create certificates keys. Only one can be installed per AS/400 system.
    - 5769-AC1 40-bit key length
    - 5769-AC2 56-bit key length
    - 5769-AC3 128-bit key length

On the AS/400 system from which you install SSL on the Express client:

- **5769-XE1: Client Access Express for Windows.** This allows your PC to download the client encryption option.
- **5769-CEx: Client Encryption.** The value "x" determines the maximum key length permitted for cryptographic algorithms. These clients are required to be downloaded on PCs running Client Access Express for Windows. You will have to install these clients from the AS/400 system. You can install the three Client Encryptions on the AS/400 system, but only one can be installed per PC:
    - 5769-CE1 40-bit key length
    - 5769-CE2 56-bit key length
    - 5769-CE3 128-bit key length

On the Microsoft Windows PC system:

- **5769-XE1 Client Access Express for Windows.** This software can be installed in different ways, from the AS/400 system, from a CD containing the product, etc. But it needs to be installed first before downloading the Client Encryption software from the AS/400 system.

Both cryptographic products (on the AS/400 and the PC system) have been broken down into three different products with different encryption key lengths. This is due to the fact that cryptography is country independent and while some countries accept 128-key encryption, other only accept 40-bit key. Both products on the Server (AS/400) and the client (PC) negotiate the highest encryption key length supported by both parties.

The 5769-CEx Client Encryption products (for the PC) are installed with data authority set to *PUBLIC EXCLUDE, for export regulations reasons. Remember these products are installed into the PC, from the AS/400 system. For a user, to be able to install any of these products on the PC, they need to be granted authority to one or more of the SSLxxx (where xxx = 40, 56 or 128) directories by a systems administrator.

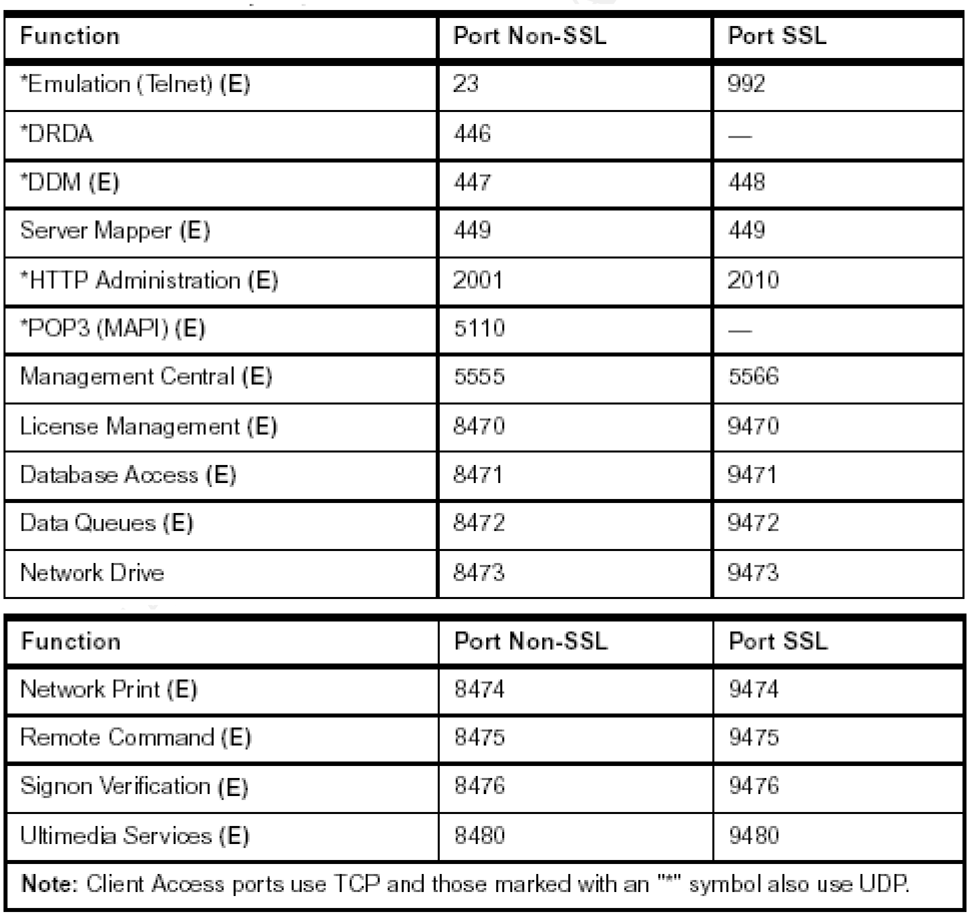
As an example, to grant ID “DAVE” authority to install the 5769-CE3 support on the PC, run the following AS/400 command:

CHGAUT OBJ(‘QIBM/ProdData/CA400/Express/SSL/SSL128’) USER(DAVE) DTAAUT(*RX)

To grant all users authority to install the 5769-CE3 support on the PC, run the following AS/400 command:

CHGAUT OBJ(‘QIBM/ProdData/CA400/Express/SSL/SSL128’) USER(*PUBLIC) DTAAUT(*RX)

When supporting SSL sessions, the AS/400 uses additional TCP/IP ports and server programs. Bellow is a list of the Client Access Express for Windows ports used, both with and without SSL communications.



Function	Port Non-SSL	Port SSL
*Emulation (Telnet) (E)	23	992
*DRDA	446	—
*DDM (E)	447	448
Server Mapper (E)	449	449
*HTTP Administration (E)	2001	2010
*POP3 (MAPI) (E)	5110	—
Management Central (E)	5555	5566
License Management (E)	8470	9470
Database Access (E)	8471	9471
Data Queues (E)	8472	9472
Network Drive	8473	9473
Network Print (E)	8474	9474
Remote Command (E)	8475	9475
Signon Verification (E)	8476	9476
Ultimedia Services (E)	8480	9480

Note: Client Access ports use TCP and those marked with an "*" symbol also use UDP.

Installing and Configuring SSL for Client Access Express

Since there are several instructions to follow before SSL can be used in Client Access Express connections, you will find a generalized form of them in this paper. It is intended to give you a bigger picture and make the whole procedure clearer. For each of the generalized steps within the whole procedure, the paper will have references to where you can find the actual instructions to carry out. The confusing part is to know when, how and why to carry out these instructions when they are located in different places on different books or manuals. This is exactly what this paper will try to clear up. These directions assume that the requirements previously mentioned are met. Please make sure this is true before continuing.

As far as the digital certificate infrastructure, the AS/400 will be considered the private Certificate Authority issuing all server certificates. Also, the same AS/400 that contains the Certificate Authority will be the host for the server applications to be secured with SSL. For each of those server applications, SSL needs digital certificate(s) to initiate SSL connections. You could have a Certificate Authority on an AS/400 system issuing digital certificates for a server application on another AS/400 system. This scenario is not within the scope of this paper.

Given the above assumptions the generalized steps to be taken are as follows:

Step 1. Install Client Encryption on the PC. Install one of the subsequent products: 5769-CE1, 5769-CE2 or 5769-CE3 on the PC client with Client Access Express for Windows already installed. Keep in mind, this is downloaded from an AS/400 system and only one of them can be installed on each PC, although all three of them might be installed in the AS/400 system. It is probably better if you install the highest possible, considering legal issues for the country in question.

The best place to find the actual instructions to follow for this step is in the IBM Redbook titled "*AS/400 Client Access Express for Windows: Implementing V4R4M0*", on page 82, section 4.3 "*Installing SSL on the Client PC*". The book code is SG24-5191-00; you will find a link to this book on-line at the references section of this paper.

Step 2. Digital Certificates on the AS/400 system. This is a long and involved step, so it has been broken down into 3 different sub-steps we will call **2a**, **2b** and **2c**. In all of these sub-steps we will be working with getting the digital certificate infrastructure ready to be used. This is done by defining the AS/400 system as our private CA, then creating and assigning certificates for the sever applications that will be protected with SSL. One certificate can be used for all server applications.

You will encounter three different types of certificates throughout this paper and its references. CA certificates are those that entities (like computers) download to allow them to trust the corresponding CA. System Certificates are those that you create and store on the AS/400 system configured as a CA. When you first define an AS/400 as a CA, it will prompt you to create a System Certificate for the AS/400, which will be setup as default. You can later create other system certificates issued by your AS/400 CA. Once you take one of the System Certificates and assign it to a specific server application on the AS/400, you have defined a Server Certificate. These are certificates related to or assigned to a server application. Hence, Server Certificates are System Certificates that have been assigned to a server application on the AS/400 system.

Before carrying out these instructions, you may need to run the following command: STRTCPSVR *HTTP *ADMIN. The HTTP Server on the AS/400 is used to run the DCM (Digital Certificate Manager), which allows for everything regarding digital certificates in the

AS/400 to take place.

Step 2a. Make the AS/400 a Certificate Authority. This step consists of three basic instructions. First, a form has to be completed with the information required to create a CA definition. Then, certificate authority policy data is required and assigned to the CA being defined. Finally, you'll need to select the system applications that will trust the CA being defined. If you do not use digital certificates issued by another CA, you may select all system applications as trustee for this CA. If you will make use of digital certificates from a different CA, besides the one being created, then try choosing only those applications you will later setup for SSL communications within Client Access Express. For example, if you will be setting up 5250 emulations with SSL communication, you will need to select "QIBM_QTV_TELNET_SERVER", the Telnet server application, to trust the CA being defined. After selecting all applications that will trust the CA being defined and confirming this selection, you'll be prompted to create a System Certificate. This step will be discussed next.

The specific instructions to follow for the definition of a CA in the AS/400 system are given in the IBM Redbook titled "*AS/400 Client Access Express for Windows: Implementing V4R4M0*", on page 477, Appendix C, Section C.2 "*AS/400 SSL Setup*". Follow the instructions numbered from 1 until 9 (included). After following these instructions, please continue to Step 2b immediately. The book code is SG24-5191-00; you will find a link to this book on-line at the references section of this paper. Notice that the example in this Appendix chooses only the Telnet Server application to trust the CA being defined. You can and might want to choose more than just that one.

Step 2b. Create a System Certificate for the AS/400 Certificate Authority. As part of the definition of a Certificate Authority in the AS/400, a system certificate has to be created. Then it will be defined as the default system certificate. In order to create the system digital certificate, another set of fields in a form has to be filled out. One of these fields is *Server name*, this value is recommended to be the TCP/IP host name of the system. It will make things easier if later you decide to use this certificate for an HTTP application. You will then be asked for the applications that will use this certificate. For our case, select the Client Access Express applications you which to protect with SSL. Last, the system digital certificate just created has to be set as the default. This same certificate will be the one used by our applications to communicate with SSL, which is created with key label *DFTSVR.

It is important to note that if you intent to have several certificates, either issued by the AS/400 CA or by any other CA as part of a more complex digital certificate infrastructure, you might want to use a different certificate rather than the default one for Client Access Express applications. As you will see, the default certificate will have a label *DFTSVR. However, certificate key labels on a particular certificate store have to be unique. If you will be having different certificates for different applications and uses, it is much easier to manage them when they have appropriate key labels. This will also facilitate the task of moving certificates between AS/400 systems, if necessary.

The specific instructions to follow for Step 2b are given in the IBM Redbook titled "*AS/400 Client Access Express for Windows: Implementing V4R4M0*", on page 480, Appendix C, Section C.2 "*AS/400 SSL Setup*". Follow the instructions numbered from 10 through 19 (included). Notice that these set of instructions follow the ones from Step 2a, meaning that they assume you come from defining a new CA on your AS/400 system. The book code is SG24-5191-

00; you will find a link to this book on-line at the references section of this paper. Again, the example used here chooses only the Telnet Server application as the only one to use the certificate being created; you might want to select more.

Step 2c. Assign a Server Certificate to application(s). Now you can assign a digital certificate to the specific server applications you want to secure. As well as to make these server applications trust the CA that issued the digital certificate.

By default, each secured server application will trust the CA that issued the digital certificate they used to communicate with. We only need to assign the certificate to each server application. In doing this, you will tell those server applications that the digital certificate assigned to them is the server certificate they will use to communicate with their clients in SSL mode.

Remember that the digital certificate you will assign to the server applications is the one created in the previous step (*DFTSVR). Every time you assign a digital certificate to a TCP/IP server application, the server application now has to listen on a new TCP/IP port for incoming requests. This means that after assigning the certificate, if the TCP/IP application server was already running on the AS/400 system, you will need to restart it. Do this by executing the following commands:

```
ENDHOSTSVR SERVER(*ALL)
STRHOSTSVR SERVER(*ALL) RQDPCL(*TCP)
```

The specific instructions to follow on Step 2c are given in the IBM Redbook titled "*AS/400 Internet Security: Developing a Digital Certificate Infrastructure*", on page 190, Section 6.2.3 "*Configuring the AS/400 system*". Follow all the numbered instructions in the section, numbers 1 until 5. The book code is SG24-5659-00; you will find a link to this book on-line at the references section of this paper. Remember to assign the certificate to all applications you which to secure.

Step 3. Allow Client Access Express on the PC client to trust the AS/400 CA. The Client Access Express for Windows software installed in your PC will be the client for the server applications at the AS/400. As part of the SSL handshake (connection setup), the server application will send its digital certificate (previously assigned to that server application) to the PC client, which contains the server application's public key and some other information for the PC client to confirm. Also in this digital certificate, the CA that issued the certificate (the AS/400 CA in this case) is specified. The PC client SSL software communicates with this CA to validate the server application's identity. Before this can happen, the PC client SSL software has to be told that the Client Access Express for Windows trusts the mentioned CA. Remember the SSL software is installed as an option on the Client Access Express for Window software.

By adding a CA certificate to the Client Access Express key database, we are telling the Client Access Express for Windows software to trust that CA. There are two basic ways to get this done. The first one is by using a tool called CWBCOSSL, which you can download for free from *http://www.as400.ibm.com/clientaccess/cadownld.htm*. This tool will allow you to download the CA certificate from the AS/400 system and add it to the Client Access Express key database, all in one step. If you don't use this tool, you will need to take two steps; first download the CA certificate from the AS/400 system into an ASCII file (the information will be encrypted) and second, add the CA certificate to the Client Access Express key database from the ASCII file created.

If you need to add the CA certificate in a considerable number of Client Access Express PCs, you may prefer to use the second method to add the CA certificate to the Client Access Express. This method is more suitable than the first for deployment on a certain number of PCs. In pursuing this method, be sure to securely save the ASCII file where you downloaded the CA certificate while you add it to different PCs. After it has been added to all PCs, it might be best to delete the ASCII file containing the CA certificate.

When working with the second method mentioned above, there are three important files in the PC that you should know about:

ikmguiw.exe: This is the program that runs the IBM Key Management. From this program you can manage key databases for Client Access Express and add CA certificates to it.

cwbssldf.kdb: This is the default key database used by Client Access Express.

cwbssldf.sth: This file contains the key database password, after you change the default password that comes with the key database (it is recommended to change the default password). In the AS/400 literature they call "stashing" the password, the process of creating a file that contains it. If you change the default password on a key database, you will be "stashing" the new password.

To run the first method, download the tool, run it and follow instructions on the screen. For the second method, there are two sets of instructions. The instructions to download the CA certificate from the AS/400 system into an ASCII file, are given in the IBM Redbook titled "*AS/400 Client Access Express for Windows: Implementing V4R4M0*", on page 85, Section 4.4 "*Downloading the Digital Certificate*". Follow all numbered instructions, from 1 to 9. The instructions to add the CA certificate from the ASCII file downloaded are given in the same book, on page 90, Section 4.5 "*Managing Certificates on Your PC*". Follow all numbered instructions, from 1 to 7. The book code is SG24-5191-00; you will find a link to this book on-line at the references section of this paper.

Step 4. Setup Client Access Express applications to communicate with SSL. Client Access Express enables SSL communications within the following functions: Operations Navigator at connection, PC5250 emulations per session (both display and printer mode supported), Data Transfers at transfer requests and ODBC at data source level. You can enable SSL for any combination of these functions.

There are three different SSL related options for PC5250 emulation sessions, Data Transfers and ODBC data sources, they are: "Do not use SSL", "Use SSL" and "Use same security as Operations Navigator connection". The latter is the default option. The advantage of using this option is that only by enabling SSL for Operations Navigator, you will be enabling SSL for the whole PC system. An advantage of at least enabling SSL for Operations Navigator at beginning (even if you disable it later) is that a check is done before to make sure that the AS/400 system you want to connect to is running OS/400 V4R4M0. When this is not the case, Operations Navigator dims the option to use SSL.

The instructions to setup SSL for Operations Navigator are given in the IBM Redbook titled "*AS/400 Client Access Express for Windows: Implementing V4R4M0*", on page 95, Section 4.6.1 "*Enabling SSL for Operations Navigator*". To setup SSL for PC5250 Sessions go to the same book, page 96, Section 4.6.2 "*Enabling SSL for PC5250 Sessions*". To setup SSL for Data Transfer go to the same book, page 97, Section 4.6.3 "*Enabling SSL for Data Transfer*". To setup SSL for ODBC go to the same book, page 99, Section 4.6.4 "*Enabling SSL for ODBC*".

Follow all numbered instructions in each case. The book code is SG24-5191-00; you will find a link to this book on-line at the references section of this paper.

When to use SSL with Client Access applications

Enabling SSL in Client Access Express degrades the performance of the communication by up to 30%. This means that you will need to think through in which situations you want to make use of SSL. You will definitely want to enable SSL if you're communication path goes through The Internet or any private network, other than yours. A VPN will be considered part of the private network you own. So, if the Client Access Express communication is done through a VPN, you might not need to enable SSL on the client. When using Client Access Express within your own private network, you might not need to enable SSL as long as privacy, integrity, authentication and non-repudiation being broken from inside users is not one of your current threats. However, something else to consider before getting away from SSL on PCs within your private network is the fact that your network perimeter has to be very well protected. You might want to make sure this is the case before taking into account other considerations.

When involving yourself with digital certificates for your systems, the task could become confusing. SSL most likely won't work well without a good digital certificate infrastructure in place. It is important to think through the design of this infrastructure before you decide to enable SSL on your network. In any case, it would be appropriate to compensate for the degradation on the performance, when using SSL. You might want to consider other ways to make up for the performance loss. Before enabling SSL, try to make sure you have set the necessary PTFs (Program Temporary Fix) both for the operating system version on the AS/400 and its products, and the operating system version on the PC. Keep in mind that every situation is a different story and that you should be in better shape by getting professional help.

References

1. IBM Corp. "APAR II11853". April 25, 2001. Accessed September 23, 2001.
http://www-912.ibm.com/n_dir/nas4apar.nsf/c79815e083182fec862564c00079d117/8bb9a04bf81593a58625677700493d2e?OpenDocument

2. IBM Corp. "APAR II12052". November 30, 1999. Accessed September 23, 2001.
http://www-912.ibm.com/n_dir/NAS4APAR.NSF/51d11a683a56a5cc862564c000763b23/2e806d64573b3d24862567ef00341d25?OpenDocument&Highlight=2,ii12052

3. IBM Corp. "SSL Client Authentication". "Telnet Server". September 23, 2001.
http://www-1.ibm.com/servers/eserver/iseries/tcpip/telnet/ssl.htm

4. IBM Corp. "AS/400 Client Access Express for Windows: Implementing V4R4M0". IBM Redbooks. SG24519100. May 1999. Accessed September 23, 2001.
http://www.redbooks.ibm.com/redbooks/SG245191.html

5. IBM Corp. "AS/400 Internet Security: Developing a Digital Certificate Infrastructure". IBM Redbooks. SG24565900. February 2000. Accessed September 23, 2001.
http://www.redbooks.ibm.com/redbooks/SG245659.html

6. Tnt400.com. “Client Access Security”. Accessed September 23, 2001. http://www.as400network.com/Resources/ClubTech/TNT400/bo400ng/client_access_security.htm

7. Tnt400.com. “Client Access Through A Proxy”. Accessed September 23, 2001. http://www.as400network.com/Resources/ClubTech/TNT400/bo400ng/AS400Q0185.htm

8. Tnt400.com. “Client Access Through The Public Internet”. Accessed September 23, 2001. http://www.as400network.com/Resources/ClubTech/TNT400/bo400ng/AS400Q0253.htm