GXS

Business Exchange Services Internet transfer User’s Guide

Version 2 Release 3

Fourth Edition (November 2005)

Contents

To the reader

This book describes how to send and receive documents using Business Exchange Services Internet transfer. This service, offered by GXS, was formerly known as Internet data and document exchange (IDDX). For brevity in this user's guide, it will be referred to as the Internet transfer service.

Related information

Users of Cyclone Interchange™ Solo should refer to the *Cyclone Interchange Administrator's Guide* for complete information on that product. The *Business Exchange Services Internet transfer User's Guide* contains only the information directly related to using the Cyclone Interchange Solo product with the Internet transfer service. For assistance with other EDIINT AS1 or AS2 certified clients, contact your software provider.

Additional publications, which may be helpful when performing the tasks described in this book, can be viewed on the Publications page of the Interchange Services for e-business Web site at http://www.gxsolc.com/edi_bes.html.

Getting help

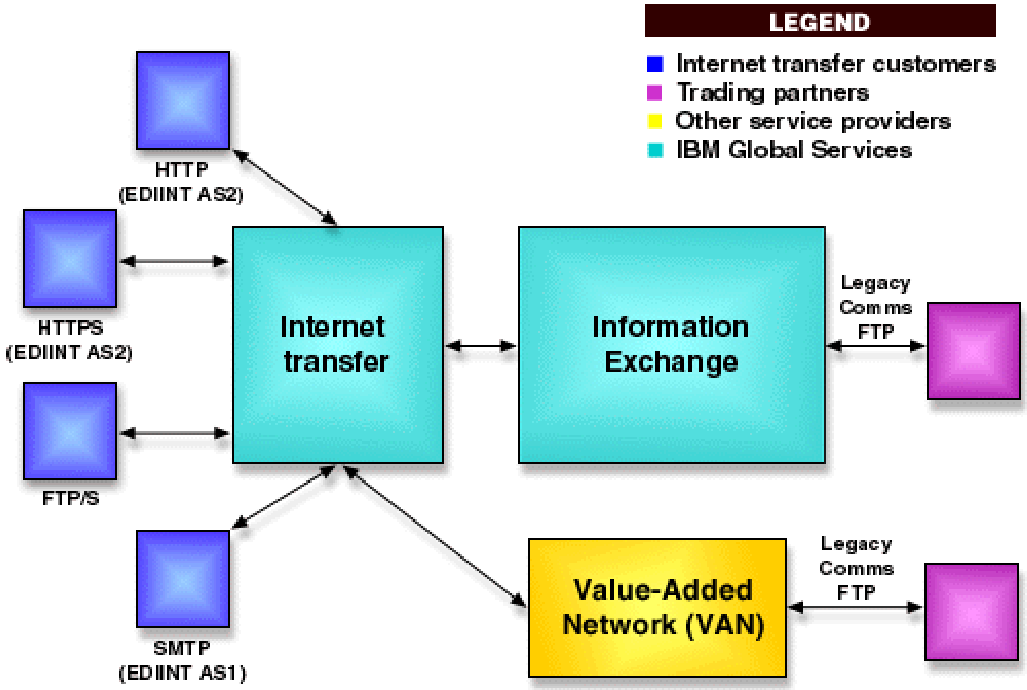
For technical assistance with the Internet transfer service, contact the GXS Community Support, toll free, at 877-326-6426 and select 6, and then 1. You can also visit our Web site at http://www.gxs.com/EDIsupport.

Chapter 1

Getting started

Users of Business Exchange Services Internet transfer can exchange documents in a security-rich environment with Internet users, Information Exchange users, and value-added network (VAN) users. The Internet transfer service supports a variety of transfer protocols and allows you the flexibility of using a protocol that is different from the one used by your trading partners. Without changing their existing system, EDI hubs can enable large numbers of trading partners who want to use the Internet.

The following diagram shows how the Internet transfer service is structured.



Selecting a transport protocol

Before you can exchange documents with trading partners using the Internet transfer service, you must determine the transport protocols that you intend to use, and then select the appropriate client software.

You can choose one transport protocol for each account. When choosing a transport protocol, consider the following:

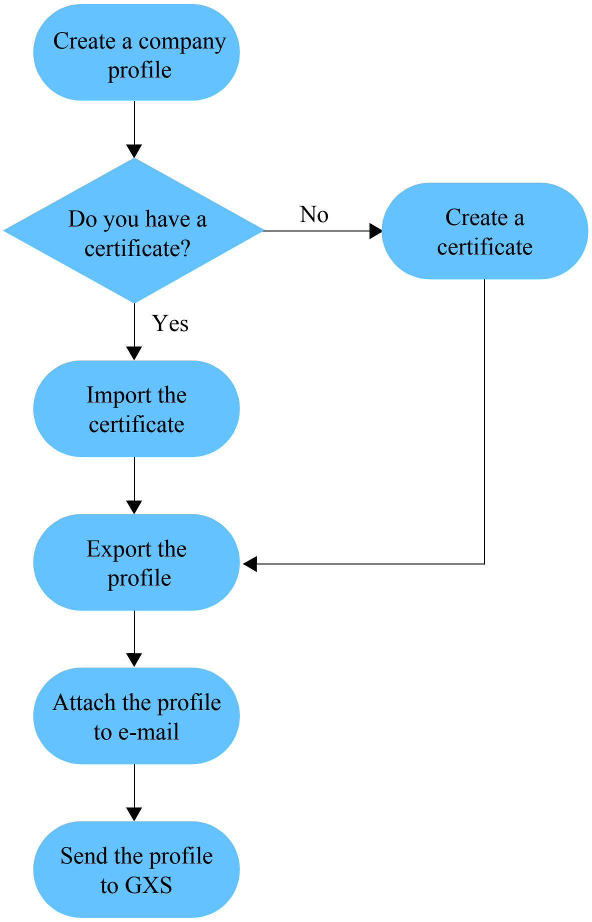
- Does the transport protocol meet your trading requirements?
- Does the transport protocol meet your organization's security policies?
- Does both your system and the Internet transfer service support your preferred transport protocol?

The following table may help you determine which transport protocol best meets your needs.

	Security	Software Required	Maximum File Size
SMTP	S-MIME certificates with encryption	Any certified EDIINT AS1 client	5 MB
HTTP/HTTPS	SSL authentication, S-MIME certificates with encryption	Any certified EDIINT AS2 client	100 MB
FTP/S	SSL authentication, session encryption	WS_FTP Pro Version 7.5T or C-Kermit Version 8.0	100 MB

Configuring HTTP and HTTPS transport with Cyclone Interchange Solo

The following diagram shows the tasks required to configure HTTP and HTTPS transport.



Creating a company profile

Create a new company profile using the Cyclone Interchange Administrator program. Refer to the *Cyclone Interchange Administrator's Guide* for detailed instructions. Use the following guidelines when creating the company name and ID:

- The company name can be a maximum of 50 uppercase, alphanumeric characters. The company name must be unique within the Internet transfer service. Uniqueness will be verified by GXS.

  For example: MYCOMPANY_APPAREL1 and MYCOMPANY_SERVICE1

- The company ID follows the same guidelines and cannot begin with a space.

Cyclone Interchange Solo settings

Tab/Subtab	Field	Value
Identity		
	Address	Your company's address
	City	Your company's city
	State/Province	Your company's state
	Zip/Postal Code	Your company's zipcode
	ISO Country Code	Your country
	Contact	Your company's contact
	Title	Contact's title
	Department	Contact's department
	Phone	Contact's phone number
	Fax	Contact's Fax number
Preferences		
	Trading Status	Active
	Alert E-mail Address	E-mail address for receiving notification of errors from the Internet transfer service
	Notify E-mail Address	E-mail address for receiving notification of undeliverable documents from the Internet transfer service
	Alert/Notify SMTP Server	Name or IP address of the SMTP mail server for the mail accounts specified for receiving Alert and Notify messages
	Inbound Backup	Backup and Delete
	Outbound Backup	Backup and Delete
	Reroute Binary Documents	Not selected

Tab/Subtab	Field	Value	
Inbound Transports			
Bundled HTTP/HTTPS			
		HTTP	**HTTPS**
	Port	4080	1443
	Authenticate	not available	selected
System Directories			
	All fields	Use default values	

Creating a security certificate

HTTPS configuration requires a security certificate that conforms to the X.509 standard. You can use Cyclone Interchange Solo to create a security certificate, or you can supply a certificate obtained from a third-party certificate authority.

Generating a security certificate with Cyclone Interchange Solo

When using Cyclone Interchange Solo, upon saving the company profile, you are given the opportunity to create a security certificate for the company.

To create a security certificate:

1. Click **Yes** when prompted to add a certificate to the Company profile.
2. Select **Generate self-signed certificate** and click **Next**.
3. Complete the following information and click **Next**.

Field	Value
Key Type	Single key
Key Length	Choose 512, 1024, or 2048. A value of 512 provides compatibility with most other systems.
Validity Period	1 - 10 years

4. Type a password for this certificate. This can be any password you like.
5. Review the information in the Summary screen. If the information is correct, click **Finish**. If changes are required, click **Back** and make the appropriate corrections.

Importing a third-party security certificate

When using Cyclone Interchange Solo, upon saving the company profile, you are given the opportunity to import an existing security certificate for the company.

To import a security certificate:

1. Click **Yes** when prompted to add a certificate to the Company profile.
2. Select **Import an existing key pair** and click **Next**.
3. Type the file name of your existing certificate. You can use the Browse button to find your certificate.
4. Type the existing password for your certificate and click **Next**.
5. Type a new password for the certificate you are creating and click **Next**.
6. Review the information in the Summary screen. If the information is correct, click **Finish**. If changes are required, click **Back** and make the appropriate corrections.

Sending your company profile to GXS

Export your company profile from the Cyclone Interchange Administration program. Your security certificate is included in the exported company profile. Send your company profile as an e-mail attachment to GXS at esg@gxs.com.

Configuring SMTP transport

You can use the Internet transfer service to send EDI documents, XML documents, and application data documents as e-mail attachments. You can use any certified EDIINT AS1 client to exchange transactions with the Internet transfer service via SMTP e-mail. Refer to the support Web site for the most current list of supported software.

Importing the GXS certificate

To import the GXS public key certificate into your e-mail program, perform the following tasks. The procedure for performing these tasks varies with each program. For detailed instructions, see the documentation for your e-mail program.

To import the GXS certificate:

1. Save the e-mail attachment containing the certificate from GXS into a folder on your system.
2. Import the certificate into your e-mail program.
3. Set security in your e-mail program to trust the certificate.

Exporting your company certificate to GXS

To export your public key certificate from your e-mail program and send it to GXS, perform the following tasks. The procedure for performing these tasks varies with each program. For detailed instructions, see the documentation for your e-mail program.

To export your company certificate:

1. Select the certificate you want to export.
2. Export the certificate to a folder on your system.
3. Send the exported file as an e-mail attachment to GXS at esg@gxs.com.

Configuring FTP/S transport

The Business Exchange Services Internet transfer FTP/S interface provides a secure FTP interface to the Internet transfer service over the Internet. This interface:

- Runs on the Business Exchange Services Internet transfer AIX platform.
- Operates in a defined and reliable manner with the supported FTP clients listed in “Selecting a transport protocol” on page 2.
- Meets the stated requirements for secure FTP function discussed in the Internet Engineering Task Force (IETF) draft document, which can be found at http://www.ietf.org/internet-drafts/draft-fordh-ftp-ssl-firewall-00.txt.

Creating a client private/public key and certificate

The FTP/S configuration requires an X.509 public key certificate signed by a third-party certificate authority (CA). You can create a public/private key pair (RSA algorithm) for your client and obtain an X.509 public key certificate from one of the CAs listed below, or you can use a key pair and public key certificate that you created previously from one of the CAs listed below.

You can create a private/public key pair and certificate using a Web browser to access a CA Web site. The following table lists the CAs recognized by the Internet transfer FTP/S service.

Certificate authority	Certificate types
BelSign NV - Belsign	Class 1, 2, 3, Secure Server
Belgacom	E-Trust Primary CA
CertPlus	Class 1, 2, 3, 3P, 3TS
Digital Signature Trust Co.	Baltimore EZ by DST
Japan Certification Services, Inc.	SecureSign RootCA1, 2, 3
Microsoft Root Authority	
RSA Data Security, Inc.	Commercial, Secure Server
Thawte Consulting	Personal Basic, Personal Freemail, Personal Premium
ValiCert, Inc.	
VeriSign, Inc.	Class 1, 2, 3

Client certificates issued by the PKI Service for Information Exchange are also accepted by the Internet transfer FTP/S service.

NOTE: If the CA you are using is not included in the above list, contact GXS.

Although the key generation/certificate, request/certificate signature procedures vary with the software and CA you use, most include the following steps.

From a CA Web site, or using FTP/S client software:

1. Generate a private/public key pair.
2. Generate a certificate request. The certificate request contains only the public key in a format, such as PKCS#10, which is recognized by a CA.
3. Submit the certificate request to a CA for a signature to obtain the signed X.509 certificate.

Importing client and server certificates to the FTP/S client

The public key certificate representing your client must be presented to the Internet transfer FTP/S server when the client connects. You must import or make the client public key certificate available on your FTP/S client software. For details on how to accomplish this, refer to the documentation for your FTP/S client software.

You can also import the Internet transfer FTP/S server public key certificate to your FTP/S client after obtaining the server certificate from GXS. This is usually not necessary, as the client should validate the server certificate automatically. You may be asked to accept the server certificate when you connect for the first time to the Internet transfer FTP/S service.

Exporting your client certificate to GXS

Before you can connect to the Internet transfer FTP/S service, you must export the public key certificate representing your client in one of the supported formats listed in the table on page 7 and send it to GXS.

To export the public key certificate for your client software and send it to GXS, you must:

1. Select the certificate you want to export.
2. Export the certificate to a folder on your system.
3. Send the exported file as an e-mail attachment to GXS at esg@gxs.com.

NOTE: The procedure for exporting a client certificate varies with each client. For detailed instructions, refer to the documentation for your client software.

Chapter 2

Exchanging documents using HTTP or HTTPS

To use HTTP or HTTPS to send data to a trading partner, you must use Cyclone Interchange Solo or another client that is EDIINT AS2 certified. Business Exchange Services Internet transfer supports secure transfer of documents using HTTP and HTTPS. HTTPS shares all the characteristics of standard HTTP with the addition of a secure socket layer (SSL) connection that provides sender authentication and an additional layer of security.

Encryption and electronic signatures are included with both HTTP and HTTPS exchanges to the Internet transfer service, and both are suitable for sending all types and sizes of documents. The additional layer of security incorporated in HTTPS is offset by reduced performance and can be a consideration when choosing between HTTP and HTTPS.

The information presented in this chapter is specific to Cyclone Interchange Solo.

NOTE: In the following instructions, you (the sender) are User1. Your trading partner is Partner1. During your configuration, replace User1 with your assigned service company ID and replace Partner1 with your trading partner's assigned service company ID. The following steps are performed using the Cyclone Interchange Administrator program.

Guidelines for exchanging documents using HTTP or HTTPS

You should be aware of the following when exchanging documents using HTTP or HTTPS:

- When exchanging documents with a VAN trading partner, only EDI (X12 and EDIFACT) data is supported.
- When exchanging documents with an Information Exchange trading partner, EDI (X12 and EDIFACT), XML, binary, and plain text data are supported.
- When exchanging documents containing X12 data with either a VAN or Information Exchange trading partner, binary segments such as BIN, S4S, and S3S cannot be used.
- When receiving documents containing XML data from an Information Exchange user, Cyclone Interchange Solo places them in the binaryin\ibm directory.

- When exchanging EDI documents with trading partners on other VANs or non-Information Exchange trading partners (IEPS/STEDI), the following hex values are not supported by the Internet transfer service as delimiters:

Direction	Segterm
Internet transfer - VANs	x0A or x0D
Internet transfer - VANs	x85 (non translatable character)
VANs - Internet transfer	x15
VANs - Internet transfer	x6A

Setting up your trading partners

Before sending documents, you must define your trading partners in your client system.

GXS (IBM partner profile) is always the primary trading partner when you are using Cyclone Interchange Solo. All documents are sent to GXS for distribution to the final recipient trading partner. Each final recipient must be defined as a secondary ID under the main GXS (IBM partner profile) trading partner ID. Contact GXS to confirm that your trading partners are defined within the service.

Defining a primary trading partner

To define GXS (IBM partner profile) as a primary trading partner:

1. Import the profile you received from GXS(IBM.pfl).

   You are prompted to select the Outbound Transports.

2. Select **Bundled HTTP** or **Bundled HTTPS**.
3. Click **Compress documents** and select a company.

   Binary trading with the selected company is now enabled.

Defining secondary IDs

You must create a secondary ID under the primary GXS (IBM partner profile) partner for each trading partner that will receive documents from you through the service.

The new secondary ID is listed in the Secondary IDs list window.

NOTE: Each partner's company ID is defined in the service system. Contact your support representative to obtain the registered ID for each trading partner.

Sending documents using HTTP and HTTPS

Once you have defined GXS (IBM partner profile) as a primary trading partner and created a secondary ID for each trading partner, you can send documents by copying the document file to the appropriate outgoing folder. The following table shows the default location of each folder. The location may be different if you have customized your installation.

Type of document	Copy to this folder
EDI	C:\CycloneSolo\data\User1\EDIOUT
XML	C:\CycloneSolo\data\User1\XMLOUT
All other	C:\CycloneSolo\data\User1\binaryout\secondary ID of partner

Receiving documents using HTTP and HTTPS

Documents sent to you from your trading partners are placed in the appropriate incoming folder.

You can check these folders for incoming documents using Windows Explorer or Cyclone Interchange Tracker. See the Cyclone Interchange Solo documentation for more information on Cyclone Interchange Tracker.

The following table shows the default location of each folder. The location may be different if you have customized your installation.

Type of document	Incoming document folder
EDI	C:\CycloneSolo\data\User1\EDIIN
XML	C:\CycloneSolo\data\User1\XMLIN
All other	C:\CycloneSolo\data\User1\binaryin\ibm

Chapter 3

Exchanging documents using SMTP

With Business Exchange Services Internet transfer, you can send documents securely using any certified EDIINT AS1 client. The e-mail message is sent to GXS with the documents attached. Refer to the support Web site for the most current list of supported software.

General guidelines for exchanging documents using SMTP

You should be aware of the following when exchanging documents using SMTP:

- When exchanging documents with a VAN trading partner, only EDI (X12 and EDIFACT) data is supported.
- When exchanging documents with an Information Exchange trading partner, EDI (X12 and EDIFACT), XML, binary, and plain text data are supported.
- When exchanging documents containing X12 data with either a VAN or an Information Exchange trading partner, binary segments such as BIN, S4S, and S3S cannot be used.
- When exchanging EDI documents with trading partners on other VANs or non-Information Exchange trading partners (IEPS/STEDI), the following hex values are not supported by the Internet transfer service as delimiters:

Direction	Segterm
Internet transfer - VANs	x0A or x0D
Internet transfer - VANs	x85 (non translatable character)
VANs - Internet transfer	x15
VANs - Internet transfer	x6A

Sending documents using SMTP

Using Bundled SMTP: once you have defined GXS (IBM partner profile) as a primary trading partner and created a secondary ID for each trading partner, you can send documents by copying the file to the appropriate folder. The following table shows the default location of each folder. The location may be different if you have customized your installation.

Type of document	Copy to this folder
EDI	C:\CycloneSolo\data\User1\EDIOUT
XML	C:\CycloneSolo\data\User1\XMLOUT
All other	C:\CycloneSolo\data\User1\binaryout\secondary ID of partner

Receiving documents using SMTP

To receive documents sent using SMTP, use the normal method provided by your EDIINT AS1 certified client for receiving messages.

Exchanging documents using FTP/S

Business Exchange Services - Internet transfer FTP/S emulates a standard, secure FTP server. Using a secure FTP client, you connect to the Internet transfer FTP/S interface using TCP/IP and submit requests using standard FTP commands.

NOTE: The FTP commands described in this chapter vary among FTP/S clients. Some clients present a graphical user interface (GUI) and the commands are implemented as menu items or buttons; other clients use different command verbs. For specific information about your FTP/S client, refer to the product documentation provided by your software vendor.

The Internet transfer FTP/S interface provides access to Internet transfer messages as if they were files on a remote file system. The Internet transfer FTP/S interface differs from a standard FTP interface in the following three ways:

- User log in requires the use of an X.509 client certificate.
- After logging on, the CD command is used to specify the user to whom files are to be sent.
- After downloading a file, the message is deleted from the system.

Connecting to the FTP/S interface

You access the Internet transfer FTP/S interface through X.509 certificates. These certificates uniquely identify users to the service and provide security while you are using the service. You must provide an X.509 client certificate to GXS prior to accessing the Internet transfer service via FTP/S. The X.509 certificate may not be self-signed.

Although the Internet transfer FTP/S service uses certificates exclusively for user authentication, FTP/S requires that you type a user ID. The Internet transfer FTP/S service verifies that the user ID matches the one provided by the X.509 certificate, unless you use the special user ID “PRIMARY”. Any password associated with the user ID (via PASS command), if sent, is accepted regardless of its value. The 230 response message shows the Internet transfer user ID corresponding to the user’s certificate.

Accessing Internet transfer FTP/S through firewalls

Using some firewall products, in certain configurations, may cause problems with secure FTP servers. This and other firewall issues are discussed in more detail in the IETF draft document, which can be found at http://www.ietf.org/internet-drafts/draft-fordh-ftp-ssl-firewall-00.txt. The Internet transfer FTP/S service runs on the standard FTP port (21).

The Internet transfer FTP/S server supports both active (server to client) and passive (client to server) mode data connections. If the FTP/S client is run from behind a local firewall, the client must use passive mode and SSL. For passive mode data connections, the Internet transfer FTP/S server uses ports 9000 - 9999 only. These ports must be opened in passive mode for client-to-server connections on your local firewall.

Listing and receiving documents

NOTE: If you are using a GUI, the client commands can be issued using buttons or drag and drop actions.

FTP/S protocol commands are shown in parentheses.

To find out if any messages are waiting to be received, use the DIR (LIST) commands from the "/ "directory to list your receivable messages. The parameters * and *.* are the only parameters allowed on the list command.

The LS (NLST) command returns a list of all the files with filenames that match the parameters along with detailed file information, including size, ownership, permissions, and dates. The LS (NLST) command returns a similar list but does not include the detailed information about each file.

For information about changing directories, see "Changing directories" on page 17.

Files are listed in the following format: *tradingpartner.filename.extension*

where:

tradingpartner is the Internet transfer ID of the trading partner that sent the message.
filename is a unique filename.
extension is the original extension of the file.

Whether referring to a secure Internet transfer FTP client or a standard FTP client, both clients use the GET (RETR) command to receive a file.

NOTE: Wildcards (*) are not allowed in the parameters for the GET command.

After a successful file transfer, a 226 reply is returned to your FTP client and the file is removed from the server. For this reason, files can only be retrieved once. Receiving a file is the only way to remove it from your list. The DELETE (DELE) command is not supported.

Sending documents

Before sending a file, change to the appropriate directory depending on whether you are sending self-routing data. See “Changing directories” below for information about self-routing data.

Send a file by using the PUT (STOR) command in your FTP/S client. After a file is sent to the Internet transfer server, a response code is returned to the client. Note that the sent file will not appear in a directory listing of remote files.

There is a 100-MB file size limit on files sent via the Internet transfer FTP/S interface. If you exceed this limit, the file is rejected, and you are sent the following error message**:** 552 Requested file action not taken. Exceeded maximum file size of 104857600**.**

After a successful file transfer, a 226 reply is returned to your FTP client. If you do not receive a 226 reply, the file was not accepted and you should resend it.

Changing directories

To change directories, use the CD command. If you are sending self-routing data, such as XML or EDI, where the recipient address is encoded within the data, then you must send the data to one of the following special directories created for this purpose:

- /XML (XML data)
- /EDI (EDI data)
- / (any self-routing data)
- /SELFROUTE (any self-routing data)

For any other types of data, such as ADF, the recipient must be explicitly stated on the CD command before sending the file. For example, to send to a trading partner whose Internet transfer service ID is INTSID, define a trading partner’s directory as /to/<INTSID>.

Other FTP commands

Other than any exceptions already described, FTP commands, generally, behave in the same way for a secure FTP server as they do for a standard FTP server, or they have been disabled. Disabled commands return a 5** error message to indicate that the command has been ignored. Following are commands that perform in a specific way with the Internet transfer FTP/S server:

- MGET and MPUT commands are supported.
- TYPE command is used to specify the data type to the FTP client and server
- Only ASCII and BINARY types are supported
- DELE and REST commands are not supported

FTP/S considerations

Although you can have more than one connection to a user's account, problems occur with simultaneous or multiple connections if conflicting commands are issued by the different sessions. If you use multiple connections, you should use one for uploading data and the other for downloading data.

ASCII versus Binary

File transfers made in ASCII mode (specifying the TYPE ASCII command prior to the transfer) result in carriage-return/line-feed character sequences being converted to just line-feed characters within the Internet transfer service and, thus, could affect ASCII to EBCDIC translations when sending data to the GXS Information Exchange service. For this reason, it is recommended that you make all file transfers in binary mode (specifying the TYPE BINARY). To prevent the ASCII to EBCDIC translation on transfers to Information Exchange, specify a filename extension of .bin on the file sent via Internet transfer FTP/S.

Chapter 5

Understanding Business Exchange Services Internet transfer security

Business Exchange Services Internet transfer provides security through a combination of certificates, encryption, authentication, digital signatures, signed receipt notices, and secure protocols as follows:

- X.509 v3 certificates for authentication of senders
- Interoperable Internet EDI (EDIINT) support
- S/MIME-based encryption and authentication
- Message Disposition Notification for signed receipts and non-repudiation of receipts
- Secure Sockets Layer (SSL) for authentication of HTTP Internet connections

Understanding public key infrastructure

Public key infrastructure (PKI) is a security architecture based on public key cryptography. Public key cryptography is based on the concept of a matched pair of keys. One of the keys can encrypt information that only the other key can decrypt. The pair of keys is designated and associated to one, and only one, trading partner. One of the keys (the private key) is only known by the designated trading partner. The other key (the public key) is published widely but is still associated with the designated trading partner.

The Internet transfer service supports the PKI method of using public key certificates. The Internet transfer service can generate, export, and import self-signed X.509 certificates, and it can import certificates from other certificate authorities as well. Regardless of the type of transport, any customer entering the Internet transfer service through the Internet must provide a certificate.

The Internet transfer service manages all certificates centrally. You are never required to directly exchange certificates with your trading partners.

How the Internet transfer service uses certificates

A certificate contains the public half of your public/private key pair along with other identifying information.

Following is some basic information about how the Internet transfer service uses certificates:

- Every company profile used to exchange secure documents must have a certificate. Cyclone Interchange Solo can generate the certificate or it can be generated externally.
- All profiles for partners with whom you exchange signed and encrypted documents must have a certificate.
- A company or partner profile can have only one active certificate at a time.
- A company or partner profile must have an active certificate to exchange signed and encrypted documents.
- A company or partner profile can have multiple valid or retired certificates.
- Certificates can be used to sign documents you transmit by all transport methods.
- When using Cyclone Interchange Solo, you can delete a certificate from the Cyclone Interchange Solo Certificates information viewer, but it remains on the system in retired status. Cyclone Interchange Solo does not use the keys in retired certificates to encrypt, decrypt, sign, or verify documents.

Limiting the risks of security exposure

Following are some recommendations to help limit the risks of security exposure:

- Do not store passwords within the e-mail client software; it makes the certificate less secure.
- Ensure machines are secure when not in use.
- Never distribute your private key certificate.
- Inform GXS when a certificate or ID is invalid.
- Contact GXS when a certificate has become compromised.
- Make use of local security measures, where possible, such as password protecting your systems and applications.

What GXS does not provide

Following are some things that GXS does not provide:

- GXS does not carry the responsibility of Certification Authority (CA).
- GXS does not check the Certificate Revocation List (CRL). Each customer is responsible to renew their own certificate, and then supply the renewed certificate to GXS.
- GXS does not distribute certificates other than its own.
- GXS is not responsible for a customer's lost or compromised certificate.

Glossary

A

application data. In the Internet transfer service, data produced by an application program that does not contain EDI or XML header information.

AS1. Applicability Statement 1 is the draft specification standard by which vendor applications communicate EDI data (or other data such as XML) over the Internet using SMTP.

AS2. Applicability Statement 2 is the draft specification standard by which vendor applications communicate EDI (or other data such as XML) over the Internet using HTTP.

C

CA. Certificate authority.

certificate. In e-commerce, a digital document that binds a public key to the identity of the certificate owner; thereby, enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority (CA).

certificate authority (CA). In e-commerce, an organization that issues certificates. The CA authenticates the certificate owner's identity and the services that the owner is authorized to use, issues new certificates, renews existing certificates, and revokes certificates belonging to users who are no longer authorized to use them.

certification authority. See certificate authority.

E

EDI. Electronic Data Interchange.

EDIFACT. EDI For Administration Commerce and Trade.

EDIINT. Electronic Data Interchange-Internet Integration.

EDI For Administration Commerce and Trade (EDIFACT). An international standard EDI format.

Electronic Data Interchange (EDI). A standard format for exchanging business data.

Electronic Data Interchange - Internet Integration (EDIINT). A standard for conducting EDI exchanges over the Internet.

Extensible Markup Language (XML). A standard meta-language for defining markup languages that was derived from and is a subset of SGML. XML omits the more complex and less-used parts of SGML and makes it much easier to (a) write applications to handle document types, (b) author and manage structured information, and (c) transmit and share structured information across diverse computing systems. The use of XML does not require the robust applications and processing that are necessary for SGML. XML is being developed under the auspices of the World Wide Web Consortium (W3C).

F

File Transport Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

FTP. File Transfer Protocol.

FTP/S. Secure File Transfer Protocol.

H

HTTP. Hypertext Transfer Protocol.

HTTPS. Secure Hypertext Transfer Protocol.

Hypertext Transfer Protocol (HTTP). In the Internet suite of protocols, the protocol that is used to transfer and display hypertext documents.

M

MIME. Multipurpose Internet Mail Extensions.

Multipurpose Internet Mail Extensions (MIME). An Internet standard for identifying the type of object being transferred across the Internet. MIME types include several variants of audio, graphics, and video.

P

private key. In computer security, a key that is known only to its owner. Contrast with public key. See public key cryptography.

public key. In computer security, a key that is made available to everyone. Contrast with private key. See public key cryptography.

public key cryptography. In computer security, cryptography in which public keys and private keys are used for encryption and decryption.

public key infrastructure (PKI). In computer security, a security architecture based on public key cryptography.

PKI. Public key infrastructure.

S

Secure Hypertext Transfer Protocol (HTTPS). A Web protocol that encrypts and decrypts Web page requests and the pages that are returned by the Web server.

Secure Sockets Layer (SSL). A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. SSL was developed by Netscape Communications Corp. and RSA Data Security, Inc.

Simple Mail Transfer Protocol (SMTP). A TCP/IP protocol used for sending and receiving e-mail.

S/MIME. A format and protocol for adding cryptographic signatures and encryption services to Internet MIME messages.

SMTP. Simple Mail Transfer Protocol.

V

value-added network (VAN). A network that provides value-added services, such as administration services, interconnection and interoperation with other services, and data security.

VAN. Value added network.

X

X12. A standard EDI format used primarily in North America.

XML. Extensible markup language.