GXS Trading Grid® Messaging Service

Connectivity Overview

A GXS Transact℠ Messaging Service for the Active Business

Table of Contents

Introduction

The GXS Trading Grid® Messaging Service (TGMS) offers a broad set of connectivity options to meet the needs of companies large and small, of varying technical levels and with different business requirements. This document provides guidance on choosing an appropriate connectivity option to best meet your company's data exchange needs.

TGMS connectivity options include:

- AS2
- AS3
- FTP
- FTPS
- SFTP
- HTTPS (scripted)
- Trading Grid Online (HTTPS)
- GXS TP Client (HTTPS)
- MQ
- OFTP
- OFTP2
- X.400

Some of these connectivity options provide similar functionality. When choosing the best option for your company, beyond meeting your minimum business and technical requirements, some of the leading decision criteria should be your familiarity, expertise and in-house technical capabilities with the connectivity solution.

If you have questions on any of these connectivity options, or on any potential option not included in this list please contact your local GXS representative. Contact details can be found on our website at *www.gxs.com/contact/*.

Trading Grid Messaging Service Connectivity Options Matrix

Connectivity Option	Client Software Options	Physical Connectivity	Security/ Authentication	Data Types
AS2	Drummond Certified recommended	Internet	Public key, SSL optional	Any (Non-EDI data types require special configuration)
AS3	Drummond Certified recommended	Internet	Public key, SSL, User ID/Password	Any (Non-EDI data types require special configuration)
FTP	Any FTP	Any method other than open Internet (examples include VPN, leased line, frame relay, etc.)	User ID/password, Additional security depends on physical connectivity	Any
SFTP	Any SFTP	Internet	SSH, User ID/password, public key (optional)	Any
FTPS	GXS-qualified FTPS software only	Internet	SSL, User ID/ password	Any
HTTPS (scripted)	Any HTTP scripting language	Internet	SSL, User ID/Password	Any
Trading Grid Online (HTTPS)	Internet Explorer or Firefox	Internet	User ID/Password, SSL	Any
GXS TP Client (HTTPS)	GXS TP Client	Internet	SSL, User ID/Password	Any
MQ	IBM® WebSphere® MQ or MQ-capable software	Closed circuit IP (leased line, frame relay, etc.) or VPN gateway	Network: VPN/IPSec or closed circuit Application: SSL	Any
OFTP	Any OFTP	X.25, ISDN, closed circuit IP (leased line, frame relay, etc.) or VPN (including ANX & ENX)	Network: VPN/IPSec, Dialup Application: SSID/Password	Any
OFTP2	Any OFTP	Internet	SSL, SSID/Password, Public key (optional)	Any
X.400	Any MTA	X.25,closed circuit IP (leased line, frame relay, etc.) or VPN	Network: VPN/IPSec Application: MTAName, Password	Any

AS2

EDIINT AS2 (Applicability Statement 2) is a specification developed as part of the IETF EDIINT Work Group that defines communication of EDI or other business-to-business data over the Internet using HTTP. AS2 provides security for the transport payload through digital signatures and data encryption. It ensures reliable delivery and non-repudiation through the use of message disposition acknowledgements (MDNs). AS2 software interoperability certification testing is performed by the Drummond Group (*www.drummondgroup.com*).

Physical Connectivity: Internet
Security: Public key, SSL optional
Receive (Push/Pull): Push
Data Types: Any (TGMS routing of non-EDI data requires special configuration)
Software Client Options: Drummond Certified clients recommended

Advantages: Real-time delivery, widespread acceptance, security and non-repudiation, utilizes the Internet
Disadvantages: Expensive software, firewall considerations

Requirements for connecting to TGMS via AS2:

- Drummond Certified AS2 software (recommended)
- X.509 certificate
- Persistent internet connection
- Server availability 24x7

Factors for considering AS2 connectivity to TGMS:

- Already have AS2 software
- Need real-time transaction exchange
- Large number of small/medium size files
- Primarily EDI data
- Considering hybrid approach (point-to-point AS2 with some partners, the rest managed through TGMS)
- Want to leverage Internet connectivity

AS3

EDIINT AS3 (Applicability Statement 3) is a specification developed as part of the IETF EDIINT Work Group that defines communication of EDI or other business-to-business data over the Internet using FTP. AS3 provides security for the transport payload through digital signatures and data encryption. It ensures reliable delivery and non-repudiation through the use of message disposition acknowledgements (MDNs). AS3 software interoperability certification testing is performed by the Drummond Group (*www.drummondgroup.com*).

Physical Connectivity: Internet
Security: Public key, SSL/TLS, User ID/Password
Receive Push/Pull: Pull
Data Types: Any (TGMS routing of non-EDI data requires special configuration)
Software Client Options: Drummond Certified clients recommended

Advantages: Security and non-repudiation, utilizes the Internet
Disadvantages: Expensive software, firewall considerations

Requirements for connecting to TGMS via AS3:

- Drummond Certified AS3 software (recommended)
- X.509 certificate
- Internet connectivity

Factors for considering AS3 connectivity to TGMS:

- Already have AS3 software
- Primarily EDI data
- Considering hybrid approach (point-to-point AS3 with some partners, the rest managed through TGMS)
- Want to leverage Internet connectivity

FTP

File Transfer Protocol (FTP) is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol (such as the Internet). Virtually every computer platform supports the FTP protocol. This allows any computer connected to a TCP/IP-based network to manipulate files on another computer on that network regardless of which operating systems are involved. There are many existing FTP client and server programs. Trading Grid FTP connectivity uses standard FTP (File Transfer Protocol, specification RFC 959) services and requires a private connection for security. Open FTP over the Internet to TGMS is not allowed. The implementation and technical details for using FTP connectivity will vary greatly depending on private connectivity option selected. Private connectivity options include:

- **VPN Security™ Remote**—Standalone PC or LAN software that provides VPN connectivity over an Internet connection. This software can be obtained through GXS.
- **VPN Security™ Gateway**—Provides host-to-host VPN connectivity via a TCP/IP connection. Requires two Internet-routable IP addresses or the ability to perform Network Address Translation (NAT) and an IPSec-compliant firewall.
- **Leased Line, Frame Relay, MPLS**—These are all examples of private, point-to-point connectivity options. These types of private connectivity options are provided by network providers such as Verizon and AT&T.
- **Dial PPP**—Dial PPP is a standard method for accessing Internet Protocol (IP)-based applications via dial up connectivity; it is available at speeds up to 56 kbps through the GXS service.

Physical Connectivity: Any method other than open Internet (examples include VPN, leased line, frame relay)
Security: User ID/Password, dependent upon physical connectivity security
Receive Push/Pull: Pull, Push (optional with some physical connectivity methods)
Data Types: Any
Software Client Options: Any FTP software

Advantages: Support for large files, can use any FTP software, security of private connection
Disadvantages: Cannot use the open Internet, firewall considerations

Requirements for connecting to TGMS via FTP:

- FTP software
- Private connectivity (VPN, leased line, frame relay, etc.)

Factors for considering FTP connectivity to TGMS:

- Familiar with FTP and use FTP for other applications
- EDI and/or non-EDI data
- Access to private connectivity options (VPN, leased line, frame relay, etc.)
- Want security of private connection versus Internet connectivity

SFTP

SFTP (SSH File Transfer Protocol) connectivity to TGMS is built upon the standard SFTP protocol as defined by the IETF SECSH working group. SFTP connectivity to the Trading Grid only supports SSH-2 protocol, which is the most typical implementation of SFTP.

SFTP connectivity to the Trading Grid Messaging Service supports SSH public key authentication and User ID/password authentication. It will first attempt SSH public key authentication and if that fails User ID/password authentication will be performed. For SSH2, either the RSA or DSA public key encryption algorithms can be used. Key lengths of 1024 (default) or 2048 are supported.

Physical Connectivity: Internet
Security: User ID/Password, SSH-2 secure shell, public key optional
Receive Push/Pull: Pull
Data Types: Any
Software Client Options: Any SFTP capable software that supports SSH-2

Advantages: Many client software options, low cost client software options, utilizes the Internet
Disadvantages: No standard support for non-repudiation, firewall considerations

Requirements for connecting to TGMS via SFTP:

- SFTP software
- Internet connectivity

Factors for considering SFTP connectivity to TGMS:

- Experienced with and already have SFTP software
- Want to leverage Internet connectivity
- EDI and/or non-EDI data
- Many client software options

FTPS

Trading Grid FTPS connectivity uses standard FTP (File Transfer Protocol, specification RFC 959) services and simply adds a secured tunnel through the Internet using Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

Qualified Client Software (as of 01/12/2011):

- Ascential™ DataStage® TX, Release 7.5 (now IBM)
- Cleo® Lexicom™ 4.1
- eBridge FTPS Communicator for GXS version 5.3
- Edisoft® Merchant™ 4.0
- Future 3—Advanced Communication Module Plus (ACM Plus)
- Inovis™ BizConnect Software, version 3.0.2.361
- nuBridges truExchange (formerly TrailBlazer ZMOD FTP Client V3R1 PTF Level PFT3100034)
- QualEDI for Windows, 32-bit version
- REIMS® B2B Frameworks version V5Re
- Robo-FTP version 3.2
- Seeburger® Business Integration Server (BIS®) Version 5.5.1

Physical Connectivity: Internet
Security: SSL/TLS, User ID/Password
Receive Push/Pull: Pull
Data Types: Any
Software Client Options: Only GXS qualified clients

Advantages: Utilizes the Internet
Disadvantages: Limited client software choices, no standard support for non-repudiation, firewall considerations

Requirements for connecting to TGMS via FTPS:

- GXS-qualified FTPS software
- Internet connectivity

Factors for considering FTPS connectivity to TGMS:

- Already have a GXS-qualified FTPS software client
- Want to leverage Internet connectivity
- EDI and/or non-EDI data

HTTPS (scripted)

HTTP is a popular request/response protocol in use every day by web browsers and web servers. Security is provided by delivering normal HTTP interaction over encrypted Secure Sockets Layer (SSL). There are many free scripting tools available, such as Perl or Ruby, that customer can use to interact with the Trading Grid via the HTTPS protocol. Unsecured HTTP connectivity to the Trading Grid is not allowed.

HTTPS connectivity to the Trading Grid further defines a subset of the header fields for routing and message handling. GXS customers using HTTPS to exchange messages through the Trading Grid must follow these specific header fields when sending and receiving documents.

Physical Connectivity: Internet
Security: SSL, User ID/Password
Receive Push/Pull: Pull or Push
Data Types: Any
Software Client Options: Any HTTPS software client or scripting language that can conform to GXS's required request header formats

Advantages: Potential for custom integration, utilizes the Internet
Disadvantages: Must conform to GXS's request header specifications, custom integration on customer side likely required, large files not supported

Requirements for connecting to TGMS via scripted HTTPS:

- HTTP scripting language and ability to create HTTP scripts
- Internet connectivity

Factors for considering scripted HTTPS connectivity to TGMS:

- Experienced with HTTP scripting
- Ability to customize internal integration
- Want to leverage Internet connectivity
- Small file sizes
- No client software costs

Trading Grid Online (HTTPS)

Trading Grid Online (TGO) provides a web-based portal interface for uploading and downloading files between you and TGMS. Once you are logged in to Trading Grid Online (TGO), you can select files for upload or download and then the files are delivered over an HTTPS connection.

Physical Connectivity: Internet
Security: User ID/Password, SSL
Receive Push/Pull: Pull
Data Types: Any
Software Client Options: Internet Explorer or Firefox

Advantages: No software costs, utilizes the Internet, simple interface
Disadvantages: Manual effort to upload and download files, not ideal for high transaction volumes

Requirements for connecting to TGMS via TGO:

- Internet Explorer or Firefox
- Internet connectivity

Factors for considering TGO connectivity to TGMS:

- Very low volumes, willing to manually upload and download files
- Want to leverage Internet connectivity
- Want to avoid any software costs

GXS TP Client (HTTPS)

GXS TP Client (TPC) is a free download available to GXS customers which provides connectivity exclusively to the Trading Grid. TPC provides a communications tool, a basic in-box/out-box interface, and a comprehensive task manager for automating and scheduling events. TPC uses HTTPS for file transfer.

Physical Connectivity: Internet
Security: SSL, User ID/Password
Receive Push/Pull: Pull
Data Types: Any
Software Client Options: GXS TP Client

Advantages: Complete GXS solution, free and easy to install
Disadvantages: No support for direct connections with other partners, no security, limited functionality

Requirements for connecting to TGMS via GXS TP Client:

- GXS TP Client software
- Windows-based PC
- Internet connectivity

Factors for considering GXS TP Client connectivity to TGMS:

- Low data volumes
- No cost for client software
- Want to leverage Internet connectivity

MQ

MQ is a connectivity option offered to customers using IBM's WebSphere MQ as a primary method of moving business documents within their business. WebSphere MQ is a widely available multi-platform message-oriented middleware software suite that provides an event-driven communication method, integrating GXS services into the client's back-end system.

Physical Connectivity: VPN Gateway, other IP connectivity (leased line, frame relay, etc.)
Security: VPN IPSec, closed circuit
Receive Push/Pull: Push
Data Types: Any
Software Client Options: IBM WebSphere MQ Manager software (MQ client not supported), JMS software that can support the IBM WebSphere MQ protocol

Advantages: Real-time, push delivery, integration directly with internal middleware system
Disadvantages: Requires IBM WebSphere MQ Manager or other MQ capable software, extensive configuration/implementation

Requirements for connecting to TGMS via MQ:

- IBM WebSphere MQ or MQ capable software
- Private connectivity (VPN, leased line, frame relay, etc.)

Factors for considering MQ connectivity to TGMS:

- Already using IBM WebSphere MQ in-house
- Access to private connectivity options (VPN, leased line, frame relay, etc.)
- Need real-time transaction exchange
- Need assured delivery features of WebSphere MQ
- Need tight integration with internal processes

OFTP

ODETTE FTP (OFTP) support is of particular relevance to the automotive sector in Europe. TGMS supports connectivity using the OFTP communications protocol, including:

- OFTP over X.25 (incl. X28)
- OFTP over ISDN (incl. X31)
- OFTP over IP (over the ENX network)
- OFTP Push—TGMS will proactively deliver data to client premises using OFTP
- VFN support—TGMS will accept data that contains a VFN (Virtual File Name) and will route the VFN with the data to OFTP or X.400 trading partners.
- ASCII/EBCDIC transliteration
- End-to-end response (EERP)

Physical Connectivity: X.25, ISDN, IP, ENX, ANX
Security: Standard network security, SSID/Password
Receive Push/Pull: Pull, Push (optional)
Data Types: Any
Software Client Options: Any OFTP client

Advantages: Reliable, stable
Disadvantages: Security, requires OFTP expertise

Requirements for connecting to TGMS via OFTP:

- OFTP client software
- X.25, ISDN, IP, ENX, ANX

Factors for considering OFTP connectivity to TGMS:

- Already using OFTP in house
- Need end-to-end delivery notifications

OFTP2

The latest version of the OFTP protocol is version 2, known as OFTP2. This version is mainly intended for secure data exchange over the public Internet, where security is guaranteed by the use of security certificates.

Physical Connectivity: Internet
Security: SSL, SSID/Password, PublicKey (optional)
Receive Push/Pull: Pull, Push (optional)
Data Types: Any
Software Client Options: Any OFTP2 client

Advantages: Internet connectivity, security, emerging standard, certified compatible client options, real time exchange option
Disadvantages: Limited acceptance outside of Europe, software costs

Requirements for connecting to TGMS via OFTP2:

- OFTP2 client software
- Internet connectivity

Factors for considering OFTP2 connectivity to TGMS:

- Already have OFTP2 software
- Need real-time transaction exchange
- Handles small and large files
- Considering hybrid approach (point-to-point OFTP2 with some partners, the rest managed through TGMS)
- Want to leverage Internet connectivity

X.400

X.400 is a suite of International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-TS) recommendations that define standards for Data Communication Networks for Message Handling Systems (MHS). X.400 is predominantly used outside of North America—for example, in retail in Europe. X400 provides a proactive or push delivery method.

TGMS supports 1984, 1988 and 1992 versions, all addressing standards and the common X.400 body parts. TGMS supports the X.400 P1 MTA protocol but not P7 Client protocol.

Physical Connectivity: X.25, IP
Security: Standard network security
Receive Push/Pull: Push
Data Types: Any
Software Client Options: Any MTA

Advantages: Reliable, international standard
Disadvantages: Security, requires X.400 expertise

Requirements for connecting to TGMS via X.400:

- X.400 MTA software
- X.25 or IP connectivity

Factors for considering X.400 connectivity to TGMS:

- Already doing X.400
- Need push delivery

NORTH AMERICA AND GLOBAL HEADQUARTERS
9711 Washingtonian Blvd.
Gaithersburg, MD 20878, US
+1-800-560-4347 t
+1-301-340-4000 t
+1-301-340-5299 f
www.gxs.com

EUROPE, MIDDLE EAST AND AFRICA
18 Station Road
Sunbury-on-Thames
Middlesex TW16 6SU
United Kingdom
+44 (0)1932 776047 t
+44 (0)1932 776216 f
www.gxs.eu

ASIA PACIFIC
Asia Headquarters
Hong Kong
GXS International
16/F China Resources Building
26 Harbour Road, Wanchai
Hong Kong
+852 2884-6088 t
+852 2513-0650 f
http://www.gxs.com.hk

GXS

About GXS
GXS is a leading provider of B2B e-commerce solutions and operates the world's largest and most expansive network of integrated business communities. The company's software and services simplify and enhance businesses process integration and collaboration among networks of trading partners. Organizations worldwide, including more than 75 percent of the Fortune 500, use GXS solutions to extend their supply chain networks, optimize product launches, automate warehouse receiving, manage electronic payments and gain supply chain visibility. Based in Gaithersburg, Maryland, GXS has operations and offices around the world. For more information, see http://www.gxs.com, http://blogs.gxs.com and http://twitter.com/gxs.