Data Transmission

User Guide

Bank of America

00-35-1993NSB

00-35-1993NSB 03-2009 – digital library number and publication date

Contents

Using the Bank of America Data Transmission Service

We are pleased that you have selected Bank of America for your treasury management services. Part of establishing your relationship is to select a method by which you will exchange information with the bank. Electronic delivery of data and images is often the most efficient and secure way to do this.

There are a number of Bank of America treasury services that utilize electronic data or image exchanges:

- Account Analysis (EDI)
- Account Reconcilement (Positive Pay, Controlled Disbursement)
- ACH (Automated Clearing House)
- Disbursement Images
- Image Cash Letter
- Information Reporting (M2M)
- Lockbox
- Receivables Network (EDI)
- The Payment Network® (EDI)

This guide summarizes the various connectivity options available for exchanging data or images electronically with Bank of America. It also describes the communication methods, security procedures, implementation components and support services available.

In addition to this guide, each treasury management service has a user guide that describes in greater detail the file formats, processing flows and security procedure requirements applicable to that service.

Getting Started

You should discuss data transmission options with your Treasury Management Representative and made a decision on which protocol you will be using. Please ensure that you have reviewed our Data Transmission Tool Kit to assist you in making a decision on a protocol. Once you have ensured that you have met the requirements of your chosen protocol, you will be contacted by an analyst from data transmission support who will work with you to set up and test your transmission.

Confirm data exchange method. After discussing data or image exchange methods with your Treasury Management Representative, you will make decisions regarding connectivity, transmission schedules, proposed testing dates, and implementation dates. You will also need to identify a technical contact who will be responsible for overseeing your transmission communications with the bank.

Installation. You will install the encryption software, communication definitions, or hardware required for the transmission method you have selected.

Exchange communication setup information. Once you have decided upon a transmission protocol and have ensured that you have all the requirements in place, a Data Transmission Analyst will begin to work with you on your transmission set up. You will be provided with information such as server address, security logon information (transmission and batch IDs) and telephone numbers.

Testing. You will then be asked to either send us a test file, or we will send you a test file depending upon the direction of your transmission. The file formats and connectivity will be validated at this time.

- Testing of the service includes both a test of the transmission protocol and security features as well a test of the file format. These tests are performed concurrently in an end to end file transfer.

Production begins. Both parties will discuss the implementation cycle and determine a production date for data transmissions. Both parties must exchange post-production contact information. Full production will not be established until both parties agree that all connectivity and file content tests have been satisfactorily completed.

The time required between initial contact and implementation of production exchanges varies depending upon the type of file exchange selected and the possible need to order, install and certify hardware and/or software.

File Formats

Please refer to the user guides for your specific treasury services for information on detailed file layout requirements.

Data Transmission Support

Bank of America uses Sterling Commerce's Connect:Enterprise® , the Sterling Integrator and Connect:Direct® products to provide centralized data and image exchange utility services.

Bank transmission systems are geographically redundant.

All systems are monitored 24 hours a day, seven days a week, 365 days a year. Availability is subject to system modification windows reserved from 11 p.m. Central on Saturday to 6 a.m. Central on Sunday.

When you call, please have your Transmission ID and if applicable, batch ID available.

Production Support	Testing Support
Technical support is available 24/7. 1.888.269.5266	Support is available on bank business days as arranged by agreement with your implementation advisor.

Electronic Access Methods

There are a variety of ways to electronically exchange data with Bank of America:

- Internet
- Value-Added Networks (VANs)

Access Control

Access to data transmission systems is controlled through the use of unique IDs and passwords.

- All transmissions use assigned IDs and passwords.
- IDs and passwords are required each time you connect to Bank of America for file exchange.
- You may receive one ID for each treasury service requested.

Integrity Control

Integrity controls are used in several ways to protect sensitive data. They can provide:

- Authentication – helps verify that the data comes from the expected sender.
- Confidentiality – encrypts data to help protect its privacy until it can be processed by the decrypting party.

While your public key is highly secure, you can enhance its security by adopting two simple measures, which experts regard as best practices:

1. Change your password every 90 days; and
2. Revoke your public key and replace it every 24 months.

Internet

You can exchange data with Bank of America over the Internet using the following methods:

- HTTPS – hypertext transfer protocol with SSL
- SSH/FTP – file transfer protocol with SSH2 encryption
- FTP/PGP – file transfer protocol with PGP encryption
- AS2 – applicability statement 2
- Connect:Direct with Secure+

Optimizing performance

To get the most out of your Data Transmission service, you may want to make a few simple adjustments that could affect performance:

- Does your ISP (Internet service provider) place limitations on the size of your file transfers? If so, please make sure that your ISP can accommodate your desired transmission.
- Do you have sufficient bandwidth to complete the transmission in less than one hour? For example, Bank of America recommends at least a T-1 equivalent connection for image transmissions.
- Do you have sufficient storage capacity for your files? Servers often manage large files better than desktop computers. Larger transmissions may exceed the amount of storage you typically allot to your company's users.

Please request a dedicated connection with sufficient bandwidth if you routinely exceed these guidelines.

HTTPS (HyperText Transfer Protocol with SSL)

Definition

HTTPS, also referred to as browser-secured file transfer, helps secure data for manual transfer over the Internet. HTTPS is an easy way to send data files over the Internet from your PC. Easy-to-use and easy-to-learn, HTTPS is often the most efficient and economical solution for businesses with moderate transmission volume. You only need an Internet connection and a browser that supports 128-bit SSL encryption.

Client Requirements

- An Internet connection.
- One of the following Web browsers to help protect the privacy of transmitted information (you do not need to purchase any additional encryption software):
    - Microsoft Internet Explorer® 6 or higher (U.S. version with 128 bit encryption)
    - Netscape® browsers 7 or higher (U.S. version with128 bit encryption)
- A willingness to manually initiate HTTPS transmissions. This user-friendly option allows you to "point and click" when transmitting data. **Automation is not recommended since technical upgrades to our Web site may interfere with your scripts**.
- The storage you will need will depend upon on the size of the files you expect to send and receive and the capacity of your desktop to store files.

Transmitting Files

- You will point your browser to our HTTPS Web site.
- Where appropriate, enter your assigned IDs and password.
- Point and click to send or receive transmissions.
- Web page indicates successful transmission.
- You will connect with Bank of America by using our Domain Name which will be provided to you during the implementation process. Bank of America uses multiple platforms for redundancy. If we need to roll over to our secondary server, by using the domain name instead of an IP address, the rollover will be transparent to you.
- You must deliver files to us, and pick up files from us.

Recommended File Size

- HTTPS limits transmissions to files of 200 megabytes or less.
- Your systems and Internet connection must allow for the transfer of your files in less than one hour.

Integrity Control

HTTPS uses 128-bit Secure Sockets Layer (SSL) encryption on the connection, using a bank-provided digital certificate to help protect privacy. User IDs and passwords are also required for exchanging files with Bank of America. These IDs and passwords are unique for each service you request.

SSH/FTP (File Transfer Protocol with SSH2 encryption)

Definition

Secure Shell FTP (SSHFTP or SFTP) is a method for encrypting information while transmitting data files over the Internet. With SSHFTP, encryption is performed during the transmission process.

- SSHFTP encrypts each packet of data in a file as it is sent over the Internet connection
- Once the packet arrives at the receiver's system, the packet is decrypted and the next packet is sent.
- The transmission is completed after all packets in the entire file have been received and decrypted.

Client Requirements

- An Internet connection.
- An FTP server or desktop client. You must use standard FTP port 22
- SSH2. The bank interoperates with many distributions that comply with the OpenSSH standard as defined by the Internet Engineering Task Force (IETF) RFC 4251.
- Bank of America supports Active and Passive FTP modes (Extended Passive is not supported)

Transmitting Files

- You will connect with Bank of America by using our Domain Name which will be provided to you during the implementation process. Bank of America uses multiple platforms for redundancy. If we need to roll over to our secondary server, by

using the domain name instead of an IP address, the rollover will be transparent to you..

- You may automate or manually initiate your FTP sessions.
- You must issue “put” commands to send or deliver data to our FTP server.
- You must issue “get” commands to retrieve data from our FTP server.
- FTP return code reports transmission status.

Recommended File Size

- SSHFTP limits transmissions to files of 200 megabytes or less.
- Your systems and Internet connection must allow for the transfer of your files in less than one hour.

Integrity Control

- We will both use SSH2 encryption to help secure data.
- Encryption ciphers supported:
    - Bank of America supports aes128-cbc, aes 192-cbc, aes 256-cbc, and 3des-cbc ciphers for encrypting files during SSHFTP transmissions.
- Message Authentication Codes supported:
    - Bank of America supports hmac-sha1 and hmac-sha1-96 message authentication codes to help protect the integrity and authenticity of transmitted data

FTP/PGP (File Transfer Protocol with PGP encryption)

Definition

FTP with PGP is a method for transmitting data and image files over the Internet using key pair encryption to encrypt the file prior to the transmission of the file.

With key pair cryptography, each pair includes a private key and a public key for encrypting messages. Your company and Bank of America exchange each other's public key. A company's private key is never exchanged.

Client Requirements

- An Internet connection.
- An FTP server or FTP desktop client.
- Ports Used:

  You must use standard FTP ports (Ports 20 and 21)

  For Image Cash Letter files, you must use port 13653.
- PGP. The bank interoperates with many distributions that comply with the OpenPGP standard as defined by the IETF RFC 2440.
- You must be able to digitally sign your PGP file.
- Bank of America supports Active and Passive FTP modes (Extended Passive is not supported)

Transmitting Files

- You will connect with Bank of America by using our Domain Name which will be provided to you during the implementation process. Bank of America uses multiple platforms for redundancy. If we need to roll over to our secondary server, by

using the domain name instead of an IP address, the rollover will be transparent to you.

- You may automate or manually initiate your FTP sessions.
- You must issue “put” commands to send or deliver data to our FTP server.
- If you use an FTP Server, you may issue “get” commands to retrieve data from our FTP Server. You may also grant us access control to “put” or deliver data to your FTP server.
- If you use an FTP desktop client, you must issue “get” commands to retrieve data since we cannot “put” or deliver data to a desktop client.
- FTP return code reports transmission status.

Recommended File Size

- FTP/PGP limits transmissions to files of 5 gigabytes or less.
- Your systems and Internet connection must allow for the transfer of your files in less than one hour.

Integrity Control

- We will both use PGP encryption to help secure data.
- We will both use digital signatures to authenticate ourselves.
- You use the Bank of America public key to encrypt the files that you send to the bank, and sign the file with your private key. Bank of America uses it’s private key to decrypt your message and verifies your signature with your public key.
- Bank of America uses your public key to encrypt files we send you and we sign the file with our private key. You use your private key to decrypt

the message we send and verify our signature using our public key.

AS2 (Applicability Statement 2)

Definition

AS2 is a file transfer protocol for automating transmissions over an HTTP or HTTPS Internet connection. It helps protect data using S/MIME for encryption and authenticates both the sender and the receiver using digital certificates.

Client Requirements

- An Internet connection.
- AS2 software. The bank interoperates with many AS2 distributions that have been certified by the Drummond Group at www.ebusinessready.org.
- A digital certificate. Digital certificates can be self-signed or authority-signed.

Transmitting Files

- You must initiate AS2 transmissions to our servers, and allow us to initiate AS2 transmissions to your servers.
- We each use digital certificates to authenticate ourselves
- AS2 generates a real time message to confirm receipt and decryption by the receiver's server.
- Unique URL's will be provided to you during set up. These URLs are unique to the service you request and are required when exchanging files.

Recommended File Size

- AS2 limits transmissions to files of 400 megabytes or less.

- Your systems and Internet connection must allow for the transfer of your files in less than one hour.

Additional Feature: Message Disposition Notification (MDN)

An MDN acknowledges successful receipt and decryption of the transmission by the receiver. The MDN is generated and returned to the sender in real time.

- **Synchronous** (sync). The MDN is sent across the same connection as the data file. That is, the sender initiates an AS2 transmission, transfers data, and then the receiver responds with an MDN.

- **Asynchronous** (async). The MDN is sent across a different connection than the data file. That is, the sender initiates an AS2 transmission, transfers data, and disconnects. The receiver then initiates an AS2 transmission and responds with an MDN.

  The bank supports both types of MDNs, but synchronous MDN is most common.

Integrity Control

- We will both use S/MIME encryption to secure data.

- We will both use digital signatures to authenticate ourselves.

Connect:Direct with Secure+

Definition

Connect:Direct with Secure+ allows companies that have Connect:Direct software to transmit encrypted files over the Internet directly instead of using a dedicated connection or virtual private network.

Client Requirements

- An Internet connection.
- Connect:Direct software for file transfer.
- Secure+ software for encryption.
- Third-party digital certificate.

Transmitting Files

- You must initiate transmissions to our Connect:Direct nodes, and allow us to initiate transmissions to your Connect:Direct nodes.
- To receive a file from Bank of America, you must supply the bank with your public Internet IP address, your node (domain) name, and your third-party registered certificate. When a file is ready for transmission, Bank of America will initiate the file transfer process by connecting to your node via the Internet and validating your digital certificate. When your node is authenticated, the file transmission begins using Secure+ to encrypt the file.
- To send a file to Bank of America, you connect to our node (domain) name and authenticate yourself with your third-party registered certificate. Once authenticated, the file transmission begins, using Secure+ to encrypt the file.

- If the transmission is interrupted, the Connect:Direct software can implement a checkpoint restart feature which allows the transmission to restart at the point of failure.

Recommended File Size

- Connect:Direct can support files up to 5 gigabytes.
- Your systems and Internet connection must allow for the transfer of your files in less than one hour.

Integrity Control

- We will both use Secure+ encryption to secure data. Encryption algorithms supported:
    - For Transport Layer Security (TLS) – preferred method
        - AES 256, AES 128, 3DES
    - For Secure Sockets Layer (SSL):
        - 3DES
- We will both use third-party digital signatures to authenticate ourselves.
    - Third party digital certificates are used for mutually authenticating both the sender and the receiver. Your certificate is authenticated to validate the identity of the sender of the file, and the host's certificate is authenticated to validate the receiver of the file. An X.509 certificate with a public key is required for both the client and the host.

Internet VPNs

Definition

An Internet VPN is a secured, private network or "tunnel" used to send and receive files with another party.

With any VPN connection, please consider the following:

- Does your anticipated file size, volume, and frequency of transmissions warrant building a VPN tunnel?
- Do you have the required software and/or hardware in house today to support a VPN?
- Can your implementation schedule afford the 6-10 weeks required for the successful conclusion of a network connectivity project?

Bank of America offers two types of VPN's as follows:

Meet-Me Internet VPN connection

- You provide the Internet VPN access and manage your Internet Service Provider (ISP).
- You build and maintain your side of the VPN tunnel.
- We build and maintain our side of the Internet VPN Tunnel.

Bank-Managed Internet VPN connection

- We purchase and install the equipment on your premise (fees apply).
- You provide the Internet VPN access and manage your Internet Service Provider (ISP).
- We build and maintain both sides of the Internet VPN Tunnel.

Client Requirements

- Internet connection. Your Internet connection should have sufficient bandwidth to complete the transmission in less than one hour.
- Connect:Direct or FTP software.
- Cisco compatible router that can support IPSec

Transmitting Files over a VPN

- Please see sections on Connect:Direct and FTP. The same process will be used via a VPN, except that the encryption (Secure+ and PGP) will not be needed as the VPN tunnel is secured.
- You can use your VPN to send all of your files to Bank of America. Your VPN can be configured to accommodate all your treasury management service needs with Bank of America. Firewall rules may need to be changed depending upon the service utilized.
- You will connect with Bank of America by using our IP Addresses which will be provided to you during the implementation process. Bank of America uses multiple platforms for redundancy, therefore a backup VPN connection is strongly recommended.

Recommended file size

- Connect:Direct or FTP over a VPN can support files up to 5 gigabytes.
- Your systems and Internet connection must allow for the transfer of your files in less than one hour.

Integrity Control

- We will both use digital certificates to authenticate ourselves.
- We will both use IPSec encryption to help secure data. IPSec requirements:
    - Encapsulating Security Payload (ESP) using 3DES 168 bit key, AES-192, or AES-256 strength encryption algorithms.
    - Encryption keys: Symmetric keys: AES, 3DES; Asymmetric keys: RSA, Elliptical Curve
    - Hashing Algorithms: SHA-1 (160 bit), SHA 224, 384, 256, or 512; HMAC-SHA1. HMAC-MD5 is not preferred.
    - Digital Signatures: RSA, DSA, ECC

Value Added Networks (VANs)

Bank of America supports file delivery over GXS.

- Other VANs are available through interconnect functionality.

- VAN's are primarily used for EDI Services. Please refer to the chart below to determine if a VAN is offered for the Treasury Management product you will be using.

Summary of Options

Bank of America offers a standard set of communication options on its centralized file exchange utility platforms. In selecting your transmission delivery solution, you will need to consider:

- The lead time required for design, engineering, ordering and installation activities
- The volume, frequency and duration of your transmission with the bank

Systems are monitored 24 hours a day, seven days a week, 365 days a year. Availability is subject to system modification windows reserved from 11 p.m. Central on Saturday to 6 a.m. Central on Sunday.

Chart of Options

These are basic set-up attributes of electronic access methods for our treasury services:

Your implementation requirements (all method require an Internet connection):

	Software requirements	Implementation lead time*
HTTPS	• Web browser - Microsoft® Internet Explorer® 6 or higher and Netscape® browsers 7 or higher • Encryption provided on the web site by the bank	1- 5 business days
SSHFTP (sFTP)	• FTP software • SSH software - SSH package that complies with the OpenSSH standard as defined by the Internet Engineering Task Force RFC 4251	1 – 5 business days
FTP with PGP	• FTP software • PGP software - PGP software that complies with the OpenPGP standard as defined by the Internet Engineering Task Force RFC 2440	1 – 5 business days
AS2	• AS2 (includes S/MIME) • AS2 software that is certified for interoperability by Drummond Group • Digital Certificate	1 – 5 business days
Connect:Direct with Secure+	• Connect:Direct software (Sterling Commerce) • Secure+ software (Sterling Commerce) • Third Party Digital Certificate	New Connect:Direct Node: 2-4 weeks New file on existing node: 5 business days
VAN	• VAN specific	VAN Specific
VPN	• FTP or Connect:Direct Software • IPSec-compatible VPN router (Cisco Compatible)	6 – 10 weeks

*Note: Please allow additional time to test file formats.

Recommended Options

These communication options are recommended for our treasury services:

	HTTPS	SSHFTP	FTP/PGP	AS2	Connect: Direct with Secure+	VPN	VAN
Account Analysis – EDI	✓	✓	✓	✓	✓	✓	
Account Reconcilement	✓	✓	✓	✓	✓	✓	
ACH	✓	✓	✓	✓	✓	✓	
Disbursement Images			✓		✓	✓	
Image Cash Letter			✓		✓	✓	
Information Reporting – M2M	✓	✓	✓	✓	✓	✓	
Lockbox – data	✓	✓	✓	✓	✓	✓	
Lockbox - Image			✓		✓	✓	
Receivables Network – EDI		✓	✓	✓	✓	✓	✓
The Payment Network® – EDI		✓	✓	✓	✓	✓	✓

Note: While VPN's can be used for any service, consideration should be given to timeframes when choosing this option.

Glossary

Terms and definitions have been gathered from the public Internet.

AS2 (EDIINT AS2)
Applicability Statement 2, or EDI over the Internet. AS2 is the standard by which vendor applications communicate EDI or other data over the Internet using S/MIME and HTTP/HTTPS.

Authentication
A process, generally a mathematical algorithm, whereby the receiver of a digital message can verify the identity of the sender.

Bandwidth
Measurement for the amount of data that can be sent through a connection. It is usually measured in bits-per-second. A full page of English text is about 16,000 bits. A fast modem can move about 15,000 bits in one second. Full-motion full-screen video requires roughly 10,000,000 bits-per-second, depending on compression.

Byte
A set of bits that represent a single character. There are usually 8 bits in a byte.

Decryption
The process of transforming ciphertext into readable text.

Digital Certificate
A digital certificate is a vehicle for the management and distribution of public keys. It binds a public key to identity information about the owner of the key. A digital certificate contains a public key, identity information, and one or more signatures to provide a chain of verification and to help prevent tampering. Public key cryptography is based on key pairs. A key pair contains a private key and a public key. Anything encrypted with one key can be decrypted only with the other key.

Digital Signature
A transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can determine whether

- the transformation was created using the private key that corresponds to the signer's public key
- the message has been altered since the transformation

EDI (electronic data interchange)	An American National Standards Institute (ANSI) defined group of transaction sets that standardize and facilitate corporate to corporate trade communications as well as enable financial transactions via the ACH, check and Wire Transfer.
Encryption	The process of transforming plain text data into an unintelligible form (ciphertext) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).
Encryption algorithm	A mathematical formula used to encrypt or decrypt a string of text.
Firewall	A combination of hardware and software that separates a LAN (Local Area Network) into two or more parts for security purposes.
FTP (file transfer protocol)	Method of transmission for the delivery of files over the Internet. FTP uses the de facto standard, TCP/IP (Transmission Control Protocol/Internet Protocol) as the transport layer for the transmission of data.
Host	Any computer on a network that is a repository for services available to other computers on the network.
HTTPS (secure hypertext transfer protocol)	Hypertext transfer protocol (HTTP) is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. Secure HTTP uses the Secure Sockets Layer (SSL) of TCP/IP to encrypt the messages.
Internet	A worldwide system of PCs connected to Servers that can communicate with other Servers.
IP (Internet protocol)	A fundamental protocol in TCP/IP networks that addresses and delivers data across the Internet.
IPSec (IP Security)	A set of protocols that supports the secure exchange of packets at the IP layer, IPSec is typically used in conjunction with a VPN. It supports two encryption modes: Transport, which encrypts the data of each packet and Tunnel, which encrypts the header and the data. IPSec uses public key exchange to support authentication and digital certificates.

Key	A single numeric value that is part of an algorithm for encrypting text.
Key Pair	A private key and its corresponding public key. The public key can verify a digital signature created using its corresponding private key. Depending upon the type of algorithm implemented, key pair components can encrypt and decrypt information for confidentiality. The private key uniquely can reveal information encrypted by using the corresponding public key.
Network	Two or more computers that are connected so they can share resources.
Node	Any single computer connected to a network.
PGP	Pretty Good Privacy (PGP) is a technique developed by Phil Zimmerman for encrypting messages. PGP is one of the most common ways to protect messages on the Internet because it is effective and easy to use.
Private Key	The secret key used in an asymmetric or public key cryptography system. It is mathematically related to the public key. Messages or signatures encoded with private keys may be decoded only with the corresponding public key, and vice versa.
Protocol	In data transmission terminology, a known industry standard used to send data so that the receiving site can interpret the data correctly.
Public key	In asymmetric encryption, the key that a user allows the world to know. It can encrypt or decrypt data for a single transaction but cannot do both.
Signature	A method that is used or adopted by a document originator to identify him- or herself to the recipient.
SSH2	Secure Shell (SSH) is a protocol that helps provide secure encrypted communications between two hosts. An SSH server listens on the standard TCP port 22.
SSL (Secure Sockets Layer)	A technology developed by Netscape which facilitates encrypted transactions between compliant browsers and Web servers.

TCP/IP (transmission control protocol/Internet protocol)	This is the suite of protocols that defines the Internet. Originally designed for the UNIX operating system, TCP/IP software is now available for every major computer operating system. To be truly on the Internet, your computer must have TCP/IP software.
VAN (value-added network)	VANs utilize a process called “mailboxing,” which removes the need to customize protocols for data transmission when a client communicates with multiple parties. The client puts a file in a mailbox using standard data communications processes; the other parties access the mailbox to retrieve the data using their own standard data communications process.
VPN (virtual private network)	A network setup solely for the users of one organization. The network may use the Internet for connectivity or have a gateway to the Internet.