KeyBank

Overview

Transmission Toolkit

Revised (June, 2023)

This publication is designed to provide accurate information about the subject matter covered. Please be aware that changes to the information may occur after the publication date.

1. Overview

Transmissions / File Transfers allow clients to automate and streamline the delivery and receipt of information reporting, payment origination and payment remittance files. This can save you time and money versus manually entering payment data, or manually retrieving information reporting / remittance data.

KeyBank provides both attended and unattended file delivery services and can exchange files that may be compatible with a variety of Treasury Management Workstations (TMS), Enterprise Resource Planning systems (ERP) and some industry specific applications. Transmissions provide a simple and secure method for sending and/or receiving files with KeyBank. Key supports three standard methods (protocols) to send and/or receive data:

1. KeyNavigator File Transfer Module (commonly referred to as "web-based file transfer")
2. Secure File Transfer (commonly referred to as a "Direct Transmission" – FTP, sFTP, AS2)
3. SWIFT for Corporates "FileAct"

Each transmission option is described in more detail in the "Transmission Options" section.

The following types of files can be sent to KeyBank:

- ACH Credit / Debit Origination Files
- ACH Control Totals Files
- Batch Wire Transfer Files
- Cash Vault Order Files
- Check Issue Files (for ARP, Positive Pay and Check Outsourcing)
- Consolidated Payables Files (transmission connection is with FIS, our Con Pay partner)
- Digital Disbursements
- E-Bill & Collect Files
- E-Lockbox Files
- EDI Origination Files (820 for ACH / Wires and 828 for Check Issues)
- Image Cash Letter Files
- Lockbox Stop Files

The following types of files can be sent to you from KeyBank:

- Account Reconcilement (ARP) Data Files
- Account Reconcilement (ARP) Paid Check Image Files
- ACH Returns and Notification of Change (NOC) Files
- BAI2 Files (Previous Day and Intraday)
- Digital Disbursements
- E-Bill & Collect Files
- E-Lockbox Files
- EDI 820 Remittance Files (Previous Day and Intraday)
- EDI 822 Account Analysis Files
- Lockbox Detail & Image Files
- Image Cash Letter Files
- Integrated Receivables Files
- Returned Items Files (data and/or images)

A list of transmission products available is found on the next page.

Transmission Products Available

Product / Solution	Transmission Methods Supported
Account Reconcilement (ARP)	• KeyNavigator File Transfer (web-based file transfer) • Secure File Transfer (Direct Transmission) • SWIFT FileAct
Account Reconcilement (ARP) - Paid Check Images	• Secure File Transfer (Direct Transmission)
ACH	• KeyNavigator File Transfer (web-based file transfer) • Secure File Transfer (Direct Transmission) • SWIFT FileAct
BAI2 (Information Reporting)	• KeyNavigator File Transfer (web-based file transfer) • Secure File Transfer (Direct Transmission) • SWIFT FileAct
Cash Vault Orders	• Secure File Transfer (Direct Transmission)
Consolidated Payables	• Secure File Transfer (Direct Transmission)* • Consolidated Payables Portal Upload* *connection is with FIS, our Con Pay partner
Digital Disbursements	• Secure File Transfer (Direct Transmission)
E-Bill & Collect	• Secure File Transfer (Direct Transmission)
E-Lockbox	• Secure File Transfer (Direct Transmission)
EDI	• KeyNavigator File Transfer (web-based file transfer) • Secure File Transfer (Direct Transmission) • SWIFT FileAct
Integrated Receivables	• KeyNavigator File Transfer (web-based file transfer) • Secure File Transfer (Direct Transmission) • SWIFT FileAct
Lockbox Data	• KeyNavigator File Transfer (web-based file transfer) • Secure File Transfer (Direct Transmission)
Lockbox Images	• Secure File Transfer (Direct Transmission)

Returned Item Data	• KeyNavigator File Transfer (web-based file transfer) • Secure File Transfer (Direct Transmission)
Returned Item Images	• Secure File Transfer (Direct Transmission)
Wire Transfer	• KeyNavigator File Transfer (web-based file transfer) • Secure File Transfer (Direct Transmission) • SWIFT FileAct

2. Implementation & Service Information

Roles & Responsibilities

The process to establish transmission services with KeyBank consists of three phases:

1. Connectivity set-up and testing
2. Application file testing
3. Move to Production (live)

Operational and technical contacts from both your organization and KeyBank will partner to ensure network connectivity is successfully set up. Your organization will then collaborate with KeyBank's personnel to test and validate file formats. Once in production, the initial transmission will be verified for completeness.

KeyBank will not supply any code or programs other than the parameters that are necessary for interaction with the bank's transmission platform(s). It is your responsibility to configure your system or application to connect with KeyBank's file transfer system.

Prior to the request for transmission services

1. You must meet all hardware and software specifications described in this toolkit. If any of the hardware and/or software specifications cannot currently be supported by your organization, you may request a technical review session with KeyBank's Transmissions Team by contacting your Treasury Services Payment Advisor.

2. You must have the appropriate staff (technical or otherwise) available to work with KeyBank to establish communication, test file formats, and run validity checks.

3. Each product type (ACH, ARP, etc.) has its own file format. Please refer to the specific applicable product file format document for details. If not already provided, your Payment Advisor can provide these to you. The test file requirement applies to all clients who will be **sending** files to KeyBank for processing. If your system or application cannot create a file in the standard format, Key can evaluate our ability to translate the incoming file from your system into the applicable product's file format for processing in our system – additional fees apply. Any questions regarding the creation of test files can be directed to your Treasury Services Payment Advisor.

4. Your internal applications must be capable of accepting files from KeyBank if you will be receiving an outbound file from KeyBank. Each product type has its own file format. Please refer to the specific applicable product file format document for details. If not already provided, your Payment Advisor can provide these to you. This requirement applies to all clients who will be **receiving** files from KeyBank. If your system or application cannot ingest a file in the standard format, Key can evaluate our ability to translate the outgoing file from our system into your system's file format – additional fees apply. Please contact your Treasury Services Payment Advisor with any questions regarding the receipt of files.

Requesting Transmission Services

1. Your Payments Advisor will work with you to determine which method of file exchange will best suit your company's needs. In most cases, your company's technical resource will have a desired transmission protocol they want you to use.

2. Your Payments Advisor will provide you with a **Secure File Transfer Request Form** to complete. This form will provide specific configuration details for our transmission protocols (IP Addresses, URLs, Port Numbers, etc.). It will also capture applicable information from you that is required to set-up and test transmission connectivity, etc.

3. Once the form and all required information has been provided to your Payments Advisor, the Transmission implementation process will begin.

Implementation Process

1. After the transmission setup forms and all necessary agreements have been received, the technical contact for your company will receive an email notifying them to expect a call from a Transmission Onboarding Specialist. Transmission Toolkit information will be included with the email. Sections of the toolkit that should be reviewed prior to the call will be identified.

2. A Transmission Onboarding Specialist will call your technical contact. During the call, the Transmission Specialist will verify the information on the set-up form and discuss the following components of the implementation process:
   a. Client commitment, responsibilities, and scheduling
   b. Formatting requirements
   c. Submitting and retrieving test files
   d. Any questions and concerns that exist

3. After the call, you will be emailed logon and sign-on credentials / instructions.

4. During the initial set-up phase, a process called the "handshake" takes place. This is the initial communication test between your organization's systems and KeyBank. This test establishes that you can communicate electronically with KeyBank. It is done before a test file is sent or downloaded.

5. If you will be retrieving files from Key, we will transmit a test file after the "handshake" process has been completed and verified. You will need to retrieve and examine the file to ensure that it meets defined requirements. KeyBank must receive confirmation from you that the file is satisfactory before transmission services begin.

6. KeyBank will work closely with your technical resources during the testing and approval phase. The pertinent individuals at your organization MUST make themselves available to work with KeyBank during the transmission set-up and testing process. The start of your selected service(s) will be delayed until the testing process has been completed.

7. Depending on the availability of your technical resources and the validity of the test file(s), completion of the entire process can take between three to six weeks.

Post Implementation

1. Once testing is complete and you confirm that the service is setup correctly, your organization will be moved from the test environment to the production environment. Once you have been moved to the production environment, you must use the same format for all files transmitted to the bank.

2. There is no limit on the number of files that you can send per day to KeyBank. Depending on the service, files will be processed as they are received, or the new file(s) will be appended to the original file and the entire file will be processed during nightly batch processing.

3. Multiple accounts can be sent in the same file, as long as they are in the same processing region (contact your Payments Advisor for details). If the accounts are from different "banks" within that region, then the files must include the bank number in the record layout. (These requirements will be discussed in detail during testing.)

4. You should not alter or add additional information, such as another account, to your file without notifying KeyBank. Proper procedures must be followed in order to ensure that all accounts are correctly setup, in the same layout, and appropriately formatted.

5. KeyBank cannot assist with correcting file issues caused by a problem with your organization's software. You must utilize your internal technical support or contact your software vendor to address and resolve issues.

6. Once you are set-up in production:
   - ***a.*** ***All Transmission Communication Issues*** should be directed to the PDO Helpdesk at (800) 282-1628 or PDO_Help_Desk@keybank.com.
   - ***b.*** ***All File / Application Issues*** (incorrect file, wrong format, etc.) should be directed to the PDO Helpdesk at (800) 282-1628 or PDO_Help_Desk@keybank.com.
   - ***c.*** ***If you are using KeyNavigator File Transfer***, please contact the Commercial Banking Services **Internet** Group at (800) 539-9039.

7. If you are performing any upgrades to hardware or software that is used for transmissions, you must contact the PDO Helpdesk to schedule pre-production testing in order to make certain your upgrades will not affect transmission communications and/or prevent production files from being sent and/or received. Please allow 5 to 10 business days prior to implementation for testing to be performed.

3. Transmission Options

KeyBank offers three file transmission options / protocols:

1. KeyNavigator File Transfer (commonly referred to as “web-based file transfer”)
2. Secure File Transfer (commonly referred to as a “Direct Transmission” – FTP, sFTP, AS2)
3. SWIFT for Corporates “FileAct”

All Transmission channels are available 24 hours a day / seven days a week. Please refer to the product grid at the beginning of this document for more information on which services can be supported by the transmission options listed above.

Deadlines for sending transmission files to KeyBank for processing:

File Type	Submission Deadline
ACH	9:00 PM ET
ARP	11:00 PM ET
Cash Vault Order	9:30 AM ET
EDI for ACH	9:00 PM ET
EDI for Wires	6:00 PM ET
Wires	6:00 PM ET

Times after which files can be retrieved from KeyBank:

File Type	Retrieval Time
ACH Returns	8:00 AM ET
Previous Day EDI	8:00 AM ET
Intraday EDI	7:00 AM ET, 12:00 PM ET, 5:00 PM ET and 8:00 PM ET
ARP	8:00 AM ET
Lockbox	8:00 AM ET (multiple files throughout the day)
BAI2 Intraday	8:00 AM ET
BAI2 Previous Day	8:00 AM ET (for ME-NH-VT-NY-OH-IN-MI) 10:30 AM ET (for CO-UT-ID-OR-WA) 11:30 AM ET (for AK)
Return Items	8:00 AM ET

4. Key Navigator Web Based File Transfer

The KeyNavigator File Transfer module allows you to upload or download data files to/from KeyBank's transmission platform using a PC and Internet browser.

KeyNavigator is a web-based system, so there's no need to use special software. You can access KeyNavigator from any Internet-enabled PC. For optimal performance, we advise that you only use versions of Browsers and Operating Systems that are currently supported by the manufacturer. This does not mean that older versions of Browsers and Operating Systems will not work with KeyNavigator; it means that they may not work as well, or as efficiently, or certain functions may not operate as intended. To determine compatibility, a technical review may be arranged by contacting the Commercial Banking Services **Internet** Team at 1-800-539-9039.

The KeyNavigator File Transfer module provides status and history for submitted and retrieved files. Files are downloadable for a period of 45 days. After 45 days files are deleted but a record of the file is available for a total of 180 days. Please visit KeyNavigator Online Help for access to User Guides, Frequently Asked Questions and Overview Tours.

5. Secure File Transfer (Direct Transmission)

Key's Secure File Transfer service allows you a simple (attended or unattended) method for processing and/or retrieving files from KeyBank. We support the following secure / encrypted transmission protocols:

*If not already provided, please ask your Payment Advisor for a copy of the "Secure File Transfer Request" form. This document provides configuration details for Direct Transmissions – IP Addresses, URLs, Port Numbers, etc. for the various protocol options.

Data Transmissions	Image Transmissions (and some select data files)
FTP w/TLS (FTPs) *PGP encryption and signing supported	FTP w/TLS (FTPs) *PGP encryption and signing supported
sFTP (SSH) *PGP encryption and signing supported	sFTP (SSH) *PGP encryption and signing supported
AS2/AS3	AS2/AS3
VPN (Secure Remote)	VPN
SWIFT for Corporates FileAct	
Other – HTTP/S, MQ Series, EBICS, VPN Private Gateway	

Please Note: Once files are retrieved, they are removed from the system. Files that are not retrieved are available on the system for 30 days.

FTP

KeyBank will only setup authenticated and encrypted FTP connections.
FTP file transfers can occur in two ways: using KeyBank's FTP Server or using a trading partner's FTP Server. KeyBank prefers that trading partners connect to our FTP Server to place/retrieve files. This gives us greater control over the connection. The options for encrypting FTP traffic are TLS or PGP.

Pretty Good Privacy (PGP) is a computer program which can be used to encrypt the payload (the file being transferred) so no one but the intended recipient can read it. PGP encryption occurs prior to sending the file. The system that receives the file must have the corresponding PGP key to successfully decrypt the file.

Transport Layer Security (TLS) is used to encrypt the traffic over the network and ensures privacy between communicating applications and their users. TLS can only occur if both the FTP Client and the FTP Server support TLS/SSL. A valid server certificate is required on the FTP Server (or FTP Proxy). TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with an encryption method. The TLS Handshake Protocol allows the parties to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. A TLS handshake occurs at connection time to establish the TLS connection.

Specific FTP Configuration Plans

- Enable TLS, but do not require (force) TLS on the FTP connection (some trading partner's may not support TLS)
- Authentication required on FTP connection (no anonymous access)
- Encryption of the payload file with PGP is required for those trading partners who cannot support TLS

AS2

AS2 is a real-time technology that provides security and encryption around the HTTP packets. AS2 file transfer is now used by many retail businesses. It has the advantage of providing built-in security features, such as support for digital signatures and encryption. AS2 specifies the means to connect, deliver, validate, and reply to (receipt) data in a secure and reliable way. Messaging features include support for MDN (Message Disposition Notice) to inform the sender of the success or failure of the file transfer. AS2 trading partners can be authenticated by the HTTP Reverse Proxy Server (SecureLink) and/or by digitally signing the message.

Specific AS2 Configuration Plans

- HTTP/S required
- Support S/MIME (default), Support digital signing of AS2 messages
- Enable basic authentication (username) for AS2 Relay in the DMZ
- Support digital signing of AS2 messages
- Enable basic authentication (username) for AS2 Relay in the DMZ