

SCHEDULE G

Secured File Transfer Protocol (SFTP) Connectivity

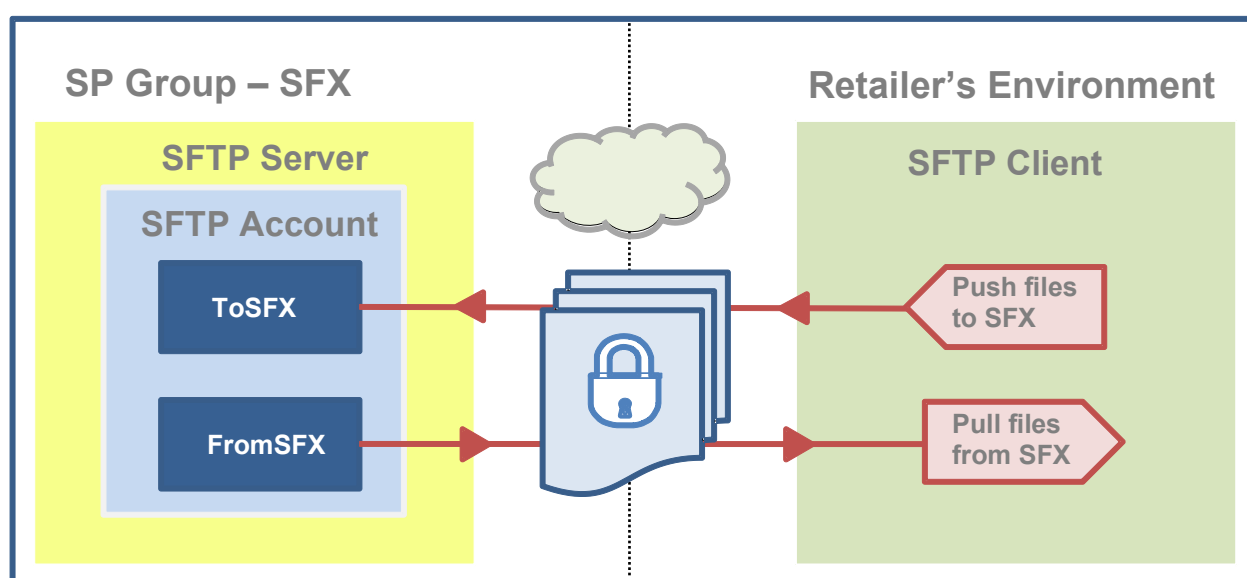
Retailer's technical team is expected to participate in the implementation on behalf of retailer and must be familiar with following terminology:

- Secured File Transfer Protocol (SFTP) connection setup
- Secure Socket Shell (SSH) keys-based authentication
- Pretty Good Privacy (PGP) file encryption

SP Group (SP) will not be able to support any connectivity query related to retailer system setup.

FILE TRANSFER APPROACH AND GUIDELINES

Following diagram summarise the file transfer approach:



- Retailer will initial connection to SP SFTP server with an SFTP account to push and pull files.
- Encryption Ciphers for SSH protocol supported: AES256-CTR and HMAC-SHA2-256.
- SSH authentication method is via public key authentication (RSA 2048-bit). There will be no password authentication required.
- All files that are transferred are encrypted with PGP keys (RSA 2048-bit or higher, trusted and signed)
- PGP Key ID should be supplied as last 16 digits.
- PGP Key Name must be less than 32 characters
- File size should not be more than 1 GB per file. Total file size per batch/transaction should not be more than 2GB.

- Each Retailer should not send more than 200 files per day. Multiple files should be compressed and zipped into one file when possible.
- Retailer should not send more than 10 concurrent file transfers at any point in time in one connection.

IMPORTANT NOTE

If any retailer is found to not following the approach and guidelines as mentioned in previous section and causes SFX SFTP Server to be overloaded, the retailer account will be disconnected from SFX to prevent other retailer's file transfer job failure. The disconnected retailer will be informed and asked to fix the issue on their side before the retailer account will be connected back to SFX for operation.

In the SFTP account for retailer, there will be 2 mailboxes - ToSFX and FromSFX

Mailbox	Permissions	Usage
ToSFX	File Upload	• Retailer to connect to SFTP server with SSH public key authentication. • The upload file is encrypted with SP's PGP public key. • Retailer to upload the PGP encrypted files to folder <u>ToSFX</u>. • Once consumed by SP, the files will not be visible in SFTP server.
FromSFX	File Download	• Retailer to connect to SFTP Server with SSH public key authentication. • The download file is encrypted with Retailer's PGP public key. • Retailer to download the PGP encrypted file from folder <u>FromSFX</u>. • Once consumed, the files will not be visible in SFTP Server.

RETAILER SFTP CLIENT DETAILS

Environment	Quality (QA)	Production
IP address	XXX.XXX.XXX.XXX (e.g 118.201.81.183)	XXX.XXX.XXX.XXX (e.g 118.201.81.183)
Port Number	XXXX (e.g 22,8122)	XXXX (e.g 22,8122)

Authentication SSH Public Key – RSA 2048-bit	Attach SSH RSA key for authentication	Attach SSH RSA key for authentication
Encryption PGP Public Key – RSA 2048-bit or higher (For SP to encrypt files send to retailer)	Attach PGP RSA key for encryption	Attach PGP RSA key for encryption

SP will provide the following SFTP Server information to retailer after receiving retailer's SFTP client details:

- SP SFTP Server Details (Hostname, IP address and Port Number)
- Retailer SFTP Account Name and mailbox
- SP PGP Public Key (For retailer to encrypt files and send to SP)

Timeline of SP providing SFTP Server information:

Environment	
Quality (QA)	3 weeks after received retailer client details
Production	3 working days after market trial completion

SYSTEM AVAILABILITY

Normal SFTP operations will minimally be between the hours of 0600 and 2200, and SP may perform SFTP system maintenance outside of these times.

Trading Partner are recommended NOT to setup polling frequency/interval setting to less than 4 hours. Every hour/minute/second polling are not allowed.

TRACKING TILL MARKET TRIAL

Planned Activities:

A. SFTP Network Connectivity, SFTP Account setup and Key exchange – QA Environment

- Retailer to share SFTP client details including SSH public and PGP public keys.
- SP to setup/create SFTP account in Server.
- SP to whitelist/open firewall port to retailer's IP address and Port.
- SP to share SFTP Server account details and PGP public key to retailer.

B. SFTP Connectivity Test – QA Environment

- Retailer to confirm access to SFTP account.
- Retailer and SP to exchange sample encrypted file via SFTP Server.
- Email sign-off from both the parties.

C. Market Trial – QA Environment

- Retailer to participate in market trial.

TRACKING AFTER MARKET TRIAL

Planned Activities:

A. SFTP Network Connectivity, SFTP Account setup and Key exchange – Production Environment

- SP to setup/create SFTP account in Server.
- SP to whitelist/open firewall port to retailer's IP address and Port.
- SP to share SFTP Server account details and PGP keys to retailer.

B. SFTP Connectivity Test – Production Environment

- Retailer to confirm access to SFTP account.
- Retailer and SP to exchange sample encrypted file via SFTP Server.
- Email sign-off from both the parties.

MISCELLANEOUS

A. Retention Period

- The files are retained (available for consumption) on SP SFTP Server for 14 days. If not consumed within retention period, it will be removed from the server.

B. Recovery Mechanism

- The files (consumed already or not consumed within retention period) can be re-enabled for consumption based on recovery request from retailer on a case-by-case basis.

C. Account Termination

- Any retailer off boarding will be followed by SFTP account termination on SP SFTP server within 14 days.

D. Automated Polling

- File polling should be aligned with the agreed and expected frequency. For instance, file with frequency set as daily should be polled once a day only or Maximum 6 times per day (Every 4 hours). Every hour/minute/second polling is not allowed.
- Re-polling is allowed for error recovery.