Cash Market

Secure File Transfer

Technical Guide

Version:	**1.3**
Prepared by:	HKEX
Date:	1 April 2020

Modification History

Version	Date	Modified By	Synopsis
1.0	18 April 2018	HKEX	First Issue
1.1	11 July 2018	HKEX	- Updated detail on supported file types - Updated restriction on SFTP file rename operations - Updated delivery time of files
1.2	24 July 2018	HKEX	- Updated description on SFTP connectivity (section 6.1)
1.3	1 April 2020	HKEX	- Updated description on Key Management on SSH Key Renewal

Table of Contents

1 Overview

1.1 Background

This document serves as a technical reference guide for data file exchange through the secure file transfer protocol (SFTP) facility provided by HKEX.

It covers the following areas of the SFTP facility:

- Access to SFTP Facility;
- Operation of SFTP Facility;
- Registration of SFTP User Account;
- Renewal of Public Keys; and
- Network configuration

This SFTP facility is used for exchange of interface files that are needed to support operation of Northbound Investor ID Model. China Connect Exchange Participants (CCEPs)/Trade-through Exchange Participants (TTEPs) should also refer to the "China Stock Connect Northbound Trading Investor ID Model System File Interface Specification" for preparation, submission and processing of Broker-to-Client Assigned Number (BCAN) and Client Identification Data (CID) files.

2 Technical Infrastructure

2.1 SFTP Standard

The SFTP facility uses industry standard SFTP and the following protocols are supported:

Protocol	RFC	Remarks
SFTP	RFC 4251-4254	Secure Shell File Transfer Protocol
SSH Public Key File Format	RFC4716	SSH2 Public Key File Format Fingerprint: MD5 message-digest

CCEPs/TTEPs are required to ensure that the SFTP client software installed in their SFTP client workstations for file submission must adhere to the above standard.

2.2 Primary and Backup SFTP Facilities

There are two sets of SFTP facilities setup at HKEX's primary and secondary data centers respectively. Under normal condition only the primary SFTP facility is in active mode. If failure occurs in the primary SFTP facility, the secondary SFTP facility will be switched into active mode.

3 Access to SFTP Facility

3.1 User Accounts

For the purpose of exchange of Northbound Investor ID files (i.e. BCAN-CID Mapping Files, BCAN-CID Response Files etc.), each CCEP/TTEP will be issued with two SFTP user accounts by HKEX for access to the SFTP facility.

Two SFTP user accounts are in the following format:

- `BN`*`nnnnn`*`001`
- `BN`*`nnnnn`*`002`

where nnnnn is the Participant ID of the CCEP/TTEP. For example, SFTP user accounts `BN01234001` and `BN01234002` would be assigned to Exchange Participant with Participant ID 1234.

CCEPs/TTEPs may use either one of the assigned SFTP user accounts together with the respective private key to login to SFTP facility for

- submission of BCAN-CID Mapping File and Authorised TTEP Firm List; and
- retrieval of BCAN-CID Response File, Authorised TTEP Firm List Response File, BCAN-CID Validation Result File and BCAN Full Image File

3.2 Secure Shell (SSH) Keys

SFTP facility adopts Secure Shell (SSH) public-key authentication. CCEPs/TTEPs need to generate a pair of SSH private and public keys, as well as a public key fingerprint, and register the said public keys together with the public key fingerprints with HKEX for each of the SFTP user accounts.

3.2.1 Public Keys

HKEX accepts RSA 2048-bit public keys in SSH2 format.

For example:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: SSH KEY
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
```

Each public key should be saved in a separate file with the following naming convention and

send to HKEX via Electronic Communication Platform (ECP) for registration:

- `BN`*`nnnnn`*`001.pub` (public key for SFTP user account `BN`*`nnnnn`*`001`)
- `BN`*`nnnnn`*`002.pub` (public key for SFTP user account `BN`*`nnnnn`*`002`)
- where *nnnnn* is the Participant ID of CCEP/TTEP.

3.2.2 Public Key Fingerprints

Public key fingerprints are MD5 hash digests of public keys in the format of 16 octets printed as hexadecimal with lowercase letters and separated by colons. For example:

```
"c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87"
```

Each public key fingerprint should be saved in a separate (text) file with the following naming convention and send to HKEX via ECP for registration:

- `BN`*`nnnnn`*`001.fpt` (fingerprint of public key for SFTP user account `BNnnnnn001`)
- `BN`*`nnnnn`*`002.fpt` (fingerprint of public key for SFTP user account `BNnnnnn002`)

SSH public keys and public key fingerprints together with the IP addresses of their SFTP client workstations used for accessing SFTP facility should be submitted to HKEX through ECP for registration. See Section 5 for details.

CCEPs/TTEPs do not need to submit their private keys to HKEX for registration.

4 Operation of SFTP Facility

4.1 Operation Hours

The SFTP facility opens for exchange of Northbound Investor ID related files from 07:00 to 22:00 on Northbound trading days.

Time	Tasks
07:00 – 15:00	Submission of BCAN-CID Mapping File and Authorised TTEP Firm List Retrieval of BCAN-CID Response File and Authorised TTEP Firm List Response File
15:00 – 18:00	Retrieval of BCAN-CID Response File and Authorised TTEP Firm List Response File
18:00 – 22:00	Retrieval of BCAN-CID Validation Result File and BCAN Full Image File

All files on the SFTP facility will be removed after 22:00. CCEPs/TTEPs should retrieve the files before 22:00. Files submission during 22:00 – 07:00 is not allowed.

CCEPs/TTEPs should also observe the service hours (schedules) of each of the BCAN system interface files as documented in the "China Stock Connect Northbound Trading Investor ID Model System File Interface Specification".

4.2 Folder Structure

Each SFTP user account has two default folders on the SFTP facility namely INBOX and OUTBOX.

Folder	Usage
INBOX	For file distribution from HKEX to CCEPs/TTEPs
OUTBOX	For file submission by CCEPs/TTEPs to HKEX
KEY_MANAGEMENT	For Public Key file submission by CCEPs/TTEPs to HKEX and result file distribution from HKEX to CCEPs/TTEPs (Fingerprint file is not necessary)

For files submission, CCEPs/TTEPs need to upload files to the OUTBOX folder.

SFTP user accounts under the same CCEP/TTEP will share the same INBOX folder. Thus both SFTP user accounts ('`BNnnnnn001`' and '`BNnnnnn002`') can retrieve same set of files from the INBOX folder for files that are distributed by HKEX.

For OUTBOX and KEY_MANAGEMENT folders, each of SFTP user account will be assigned with two individual folders which cannot be shared with other SFTP user accounts.

4.3 File Submission and Distribution

CCEPs/TTEPs submit BCAN-CID Mapping files and/or Authorised TTEP Firm List to HKEX

by uploading those files to the OUTBOX folder. After file submission, SFTP facility will collect and remove the file from OUTBOX folder.

The submitted files are validated by batch within 10 minutes during the submission window. Once files are processed by the system, they will be moved to the INBOX folder, and renamed to `XXXXX.HHMMSS.rcvd`, where `XXXXX` is the original file name and `HHMMSS` is the process time (e.g. `BCANMAPP_20180220.zip.134500.rcvd`).

Files that cannot be processed by the system e.g. incorrect file names will still be moved to the INBOX folder and renamed to `XXXXX.HHMMSS.rej`, where `XXXXX` is the original file name and HHMMSS is the process time (e.g. `BCANNNPP_20180220.zip.135100.rej`).

If response files were not delivered in 10 minutes, CCEPs/TTEPs should check again in 5 minutes intervals.

CCEPs/TTEPs should also note the following on file submission:

- Files that do not have correct file extension (i.e. "`zip`") will be rejected on submission and no "`.rej`" file will be given.
- Renaming of files (through SFTP file rename commands) that have been submitted is not supported. For instance, CCEPs/TTEPs have to ensure "file rename" (or "temporary" filename) feature of their SFTP clients (e.g. WinSCP) is turned off.

5 Registration of SFTP User Account

Once CCEP/TTEP has public key files, public key fingerprint files, and IP addresses of their client servers ready, they should put all the files together with the scanned copy of completed registration form in a single zip file and submit to HKEX via ECP for registration.

The file name of the zip file should follow the naming convention below:

- `BN`*`nnnnn`*`.zip` (where *nnnnn* is the Participant ID of CCEP/TTEP) and containing
  a. Completed Registration Form (including IP address of 2 SFTP client workstations);
  b. Public Key file name (BNnnnnn001.pub ; BNnnnnn002.pub) and
  c. Public Key Fingerprint file name (BNnnnnn001.fpt ; BNnnnnn002.fpt)

The zip file submitted previously will be overwritten by the newly submitted zip file.

DO NOT attach private keys in the zip file. CCEPs/TTEPs shall keep private keys confidential to prevent unauthorized usage.

6 Renewal of Public Keys

6.1 Procedures

CCEPs/TTEPs are advised to renew the public keys every two years. CCEPs/TTEPs should also renew the keys immediately if the private keys are compromised. CCEPs/TTEPs could renew keys during the operation hours of SFTP Facility. The key management is for normal scenario only. If any key leak or any contingency, please follow the procedure of key registration to renew the key immediately.

After generation of a pair of new SSH private and public keys for a SFTP user account, CCEPs/TTEPs have to upload new SSH public key file into the KEY_MANAGEMENT folder. The system will automatically collect the key file, import the key with validity of 730 days for the account, and then remove the key file from the folder.

File name of the public key file is highly recommended to be same as logon ID, e.g. `BNnnnnn01.pub`. Fingerprint file is not necessary in this case.

Processing result on key renewal ("Result file") will be put into the KEY_MANAGEMENT folder after the key has been imported. The result file will be named as `Result.yyyymmdd.hhmmssSSSS.success.txt` or `Result.yyyymmdd.hhmmssSSSS.failed.txt`. CCEPs/TTEPs need to refresh their SFTP client to get the result file.

It is required to renew the key for each account separately, i.e. login BNnnnnn001 to renew BNnnnnn001's key and login BNnnnnn002 to renew BNnnnnn002's key.

Under KEY_MANAGEMENT folder, it is allowed for CCEPs/TTEPs to upload public key file and Result file download, but not for file modification and deletion. Result file will be automatically removed after 10 calendar days.

6.2 Validation

The SSH public key file must be in RSA 2048-bit SSH2 format. The system will reject the key if the file format is invalid or the key length is less than 2048 bits.

The system support 2 registered SSH public keys for each account.

If the account already has 1 SSH public key registered in the system, it will allow CCEPs/TTEPs to upload a new SSH public key (2nd key), but the oldest key (the key having oldest expiration date) will be removed after 14 calendar days once the new key is uploaded and imported successfully.

If the account already has 2 SSH public keys registered in the system, it will still allow

CCEPs/TTEPs to upload a new SSH public key (3rd key), but the oldest key (the key having oldest expiration date) will be removed after 14 calendar days once the new key is uploaded and imported successfully. The system does not allow upload the 4th SSH public key.

For example, if there is only 1 SSH public key (1st key) registered in account BNnnnnn001 on 2-March, the CCEPs/TTEPs upload 2nd SSH public key on 2-March and 3rd SSH public key on 3-March. Then, 1st SSH public key will be removed after 17-March. on or before 17-March, CCEPs/TTEPs could not further upload new SSH public key to the system.

CCEPs/TTEPs cannot upload more than 5 keys within 1 hour (regardless of upload result). When they upload the 6th key, the key will be rejected and "Permission Denied" will be shown in the result file.

6.3 Result File

Processing result on key renewal is saved in the Result File. The Result file will be named as `Result.yyyymmdd.hhmmssSSSS.success.txt` if the key has been successfully processed and imported, or `Result.yyyymmdd.hhmmssSSSS.failed.txt` if the process was failed and the key was rejected. The Result file provides the file name of the uploaded SSH public key file, import date, file size and import result. failure reason will be provided if the import is failed.

Example of import success:

```
=================================================================
= File name:   A2-key-2.pub                                     =
= Import date: 2019.10.09                                       =
= File size:   477                                              =
=================================================================

Result: Success

Fingerprint:           MD5:d4:3c:cd:90:84:f5:ed:3a:bf:de:15:a6:84:e5:c6
SSH key expiry date:   2021.10.08
```

Example of import failure due to incorrect SSH public key format:

```
=================================================================
= File name:   A2-key-2.prt                                     =
= Import date: 2019.09.01                                       =
= File size:   47                                               =
=================================================================

Result: Failed

java.io.IOException: unable to parse key, format could not be identified
```

Example of import failed due to upload 4th new SSH public key:

```
================================================================
= File name:   A1-key-1.pub                                    =
= Import date: 2019.10.11                                      =
= File size:   477                                             =
================================================================

Result: Failed

Number of maximum keys 3 reached
```

6.4 Key Expiry Warning File

For each account, when a SSH key is going to expire in 14 calendar days, a warning file will be automatically generated at midnight and put into KEY_MANAGEMENT folder. The filename will be named as `SSHKeyExpireWarning_yyyymmdd.txt`.

The warning file will be automatically generated every day for SSH keys that will soon to be expired. . After the SSH public key is expired and removed, no warning file will be generated under KEY_MANGEMENT folder.

EPs are advised to check the folder regularly.

Example of warning file showing 1 SSH key to expire within 14 days:

```
Account Name:       CABC001
SSH Fingerprint:    MD5:d4:3c:cd:90:84:f5:ed:3a:bf:de:15:a6:84:e5:c6   Key Expiry Date:    2019-12-22
```

7 Network Configuration

The SFTP facility is only accessible from the Securities and Derivatives Network/2 (SDNet/2) or HKEX Service Network (HSN) which are used for connection of China Connect Central Gateway (CCCG)/Orion Central Gateway (OCG).

CCEPs/TTEPs are allowed to configure at most two SFTP client workstations. CCEPs/TTEPs need to provide the IP addresses of their SFTP client workstations to HKEX once they are available for registration.

CCEPs/TTEPs can use either one of their SFTP client workstations to connect to HKEX's SFTP facility. Both of the SFTP user accounts issued to CCEPs/TTEPs can be used on the two different client workstations.

IP addresses of SFTP clients must be within the same subnet (first 3 octets) of SDNet/2 or HSN which CCEPs'/TTEPs' trading system connects to CCCG/OCG.

7.1 Connectivity of the SFTP Facility

IP addresses of the Production SFTP facility and End-to-End SFTP Test Facility are as follows:

7.1.1 Production SFTP facility

SFTP Facility at primary data centre	SFTP Facility at secondary data centre
10.1.145.121 Port 10022 10.1.145.122 Port 10022	10.2.145.121 Port 10022 10.2.145.122 Port 10022

Connection through OCG network interface

SFTP Facility at primary data centre	SFTP Facility at secondary data centre
10.1.93.121 Port 10022 10.1.93.122 Port 10022	10.2.93.121 Port 10022 10.2.93.122 Port 10022

7.1.2 End-to-End SFTP Test Facility

Connection through CCCG network interface

End-to-End SFTP Test Facility
10.1.145.238 Port 10022 10.1.145.239 Port 10022

Connection through OCG network interface

End-to-End SFTP Test Facility
10.1.93.238 Port 10022 10.1.93.239 Port 10022