Report Retrieval Solution

For Derivatives Markets

Technical Guide

Version: 1.8

Prepared by: HKEX

Last Update: Nov 2022

Modification History

Ver.	Update Date	Section	Description
1.0	12 Sep 2018	-	First issue
1.1	Feb 2020	4.1 Operation Hours	Inserted reminder notes for report retrieval mechanism
1.2	Mar 2020	6 Renewal of Public Keys	Inserted procedures for renewal of public key
1.3	May 2020	3 Access to SFTP Facility	Inserted reminder notes for format of SFTP user accounts
1.4	Jun 2020	8 LOP Reports	Inserted LOP reports submission information
1.5	Sep 2020	2.1 SFTP Standard	Inserted reminder note for SFTP endurance feature
1.6	Sep 2021	2.1 SFTP Standard	Add SFTP Supported Key exchange algorithms, MAC algorithms and Ciphers
1.7	May 2022	4.1 Operation Hours	Update operation hours for implementation of Derivatives Holiday Trading
1.8	Nov 2022	8 LOP Reports	Remove LOP Submission features and Section 8 LOP Reports

Table of Contents

1 Overview

1.1 Background

This technical guide serves as a reference document for Clearing Participants (CPs) to retrieve DCASS and pre-trade risk management reports from HKEX through the secure file transfer protocol (SFTP) facility.

It covers the following areas of the SFTP facility:

- Technical Infrastructure;
- Access to SFTP Facility;
- Operation of SFTP Facility;
- Registration of SFTP User Account;
- Renewal for public key; and
- Network configuration

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 (Endurance feature is not supported #1)
SSH Public Key File Format	RFC4716	SSH2 Public Key File Format Fingerprint: MD5 message-digest

Below are the supported Key Exchanges algorithms, MAC algorithms, Ciphers algorithms and Public/Host Key Algorithms

Key Exchange Algorithms	curve25519-sha256@libssh.org,ecdh-sha2-nistp521, ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
MAC Algorithms	hmac-sha2-512-96, hmac-sha2-256
Ciphers Algorithms	aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
Public/Host Key Algorithms	ssh-rsa,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com

Clearing Participants (CPs) are required to ensure that the SFTP software they use for report/file retrieve must adhere to the above standard.

#1: Some CPs enabled endurance feature in their SFTP client software. Please note that endurance feature is not supported in Report Retrieval Solution, CPs should turn this feature off otherwise "Permission Denied" will be shown when attempt to upload files, e.g. SSH key.

2.2 Primary and Backup SFTP Facilities

The SFTP facility is set up at both the HKEX primary and secondary data centers. For normal operations, only the primary SFTP facility is in active mode. Under contingency situation where the primary SFTP facility becomes unavailable, HKEX will notify CPs to connect to the secondary SFTP facility.

3 Access to SFTP Facility

3.1 User Accounts

For each CP, HKEX will assign two SFTP user accounts for retrieval of DCASS and pre-trade risk management reports (i.e. RX_AUDIT, TP001 and RPI03 etc.).

The two SFTP user accounts are in the following format:
- CXXX001
- CXXX002

Where <CXXX> is the DCASS customer code of the CP. For example, CP with DCASS customer code CXYZ, two SFTP user accounts CXYZ001 and CXYZ002 would be assigned.

After registration, CPs may use either one of the assigned SFTP user accounts together with the respective SSH private key to login to the SFTP facility for retrieval of DCASS and pre-trade risk management reports.

Please note the SFTP user accounts are CASE SENSITIVE. CPs should input their SFTP user accounts **in CAPITAL LETTERS** (i.e. CP with DCASS customer code <CXYZ> should input the SFTP user account as "**CXYZ001**" or "**CXYZ002**"). CPs input user accounts in small letters cannot **login** Report Retrieval Solution.

3.2 Secure Shell (SSH) Keys

The SFTP facility adopts Secure Shell (SSH) public-key authentication. For **each SFTP user account,** CPs need to generate a pair of SSH private and public keys, as well as a public key fingerprint, and register the public key and the public key fingerprint with HKEX.

3.2.1 Public Key

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 sent to HKEX via email for registration:
- CXXX001.pub (public key for SFTP user account CXXX001)
- CXXX002.pub (public key for SFTP user account CXXX002)

Where <CXXX> is the DCASS customer code of CP.

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 sent to HKEX via email for registration:
- CXXX001.fpt (fingerprint of public key for SFTP user account CXXX001)
- CXXX002.fpt (fingerprint of public key for SFTP user account CXXX002)

SSH public keys and public key fingerprints together with the IP addresses of

their designated SFTP client workstations for accessing SFTP facility should be submitted to HKEX through email for registration. See Section 5 for details.

CPs SHOULD NOT submit their private keys to HKEX.

4 Operation of SFTP Facility

4.1 Operation Hours

Operational hours of the SFTP facility are from 07:00 to 03:30 on trading days.

All DCASS and pre-trade risk management reports will be available for retrieval via the SFTP facility within 10 calendar days after generation. CPs should retrieve and safe keep their reports in a timely manner.

Please note that there are around 60+ reports (including reports and data files for both HKCC & SEOCH) per trading day. In order to avoid causing heavily load network traffic and occupy logging of the system due to unnecessary frequent report download action, you are highly recommended to review your report retrieval mechanism through SFTP facility so as to assure reports (except RPI reports which are relating to intraday margin) are downloaded Once Every Day Only.

4.2 Folder Structure

Each SFTP user account has five accessible folders on the SFTP facility, namely COMMON and CXXX where <CXXX> is the DCASS customer code of the CP, KEY_MANAGEMENT, LOPREPORT and LOPRESULT.

Folder	Content
COMMON	Reports / files applicable to all CPs
CXXX	Reports / files applicable to designated CP <CXXX> only
KEY_MANAGEMENT	For public key renewal. Allowed for key upload and report download only, modification and deletion is not allowed. Please refer to Section 6 for details.
LOPREPORT	This folder is obsoleted. Not allowed for file upload, download, modification and deletion
LOPRESULT	This folder is obsoleted. Not allowed for file upload, download, modification and deletion.

SFTP user accounts under the same CP will access the same COMMON and

C*XXX* folders. Thus both SFTP user accounts ("C*XXX*001" and "C*XXX*002") can retrieve the same set of derivatives clearing and pre-trade risk management reports from the COMMON and C*XXX* folder distributed by HKEX.

4.3 Frequent Sign-on Control

Each SFTP user account will be restricted to a maximum of 5 times sign-on within 5 minutes. The account will be locked (unable to sign on) once it reaches 5 times within 5 minutes and automatically unlock for every 5 minutes.

For example, if a SFTP user account has signed on more than 5 times between 12:45:10 and 12:47:30, the account will be locked at 12:47:31 then unlocked at 12:50:00 automatically.

5 Registration of SFTP User Account

To register for SFTP User Accounts, CP should generate a pair of SSH keys per account; and submit their public key, public key fingerprint, and IP addresses for the designated SFTP client workstations to HKEX in a single zip file (see sample file below), together with a scanned copy of the completed registration form via email.

The file names of the zip file should follow the naming convention below:
- CXXX.zip (where <CX*XX*> is the DCASS customer code of CP) and containing

A. IP address template, filled-in with 2 IP addresses of the designated SFTP client workstations and file names of 2 Public Keys;

B. Public Key files (CXXX001.pub; CXXX002.pub) and

C. Public Key Fingerprint files (CXXX001.fpt; CXXX002.fpt)

Please open a sample zip file for reference:

Example - CXXX.zip

DO NOT attaches private keys in the zip file. CPs shall keep their private keys confidential and prevent any unauthorized usage.

6 Renewal of Public Keys

CPs are required to renew their public keys at least every two years. CPs should re-register their keys with HKEX immediately if the corresponding private keys are being compromised. See Section 5.

Self-service Renewal of Public Keys

After generation of the new SSH public and private key, CPs should renew their SSH public keys with HKEX by submitting the keys to the /KEY_MANAGEMENT folder. After submission, a result file will be generated and available for retrieval in the /KEY_MANAGEMENT folder.

CPs should take the following steps to perform self-service public key renewal:

1. Login SFTP user account, e.g. CXXX001.
2. Locate /KEY_MANAGEMENT folder.
3. Upload the newly generated SSH public key into /KEY_MANAGEMENT folder, e.g. CXXX001.pub. (Fingerprint is not necessary for public key renewal).
4. Renew SSH public key for each SFTP user account separately, i.e. log in CXXX001 to renew CXXX001's SSH public key and log in CXXX002 to renew CXXX002's SSH public key.
5. Verify the renewal result report in the same folder.

Results:

- Result file will be generated under /KEY_MANAGEMENT folder immediately[#1] after the key has been uploaded.
- The result file will be named as "Result.yyyymmdd.hhmmss.success.txt" or "Result.yyyymmdd.hhmmss.failed.txt". Error reason will be provided if import is failed.
- The result file will specify the file name of the uploaded SSH public key, import date, file size and import result.
- Result reports will be available for retrieval within 10 calendar days after generation. CPs should retrieve and safe keep their reports in a timely manner.
- New SSH public key will be effective immediately if it is uploaded successfully. The old SSH public key will be expired 14 calendar days after the new SSH public key has been uploaded.

#1: Some SFTP client software is required to refresh files list manually to show the result file.

6.1 Validity of Keys

Once the SSH public key has been successfully renewed, CPs can use either the existing or the newly generated private key to login in the following 14 calendar days. After 14 days of SSH key renewal, the existing SSH key will be expired and removed, CPs can only use the newly generated private key (pair with the public key just used for renewal) to login.

The validity of renewed public key is 730 days, expired SSH key will be automatically removed, i.e. SFTP user account cannot login if SSH key is not renewed before the expiry date. In this case, CPs are required to follow Section 5 to re-register the public key again with HKEX.

For example, a SFTP user account e.g. CXXX001, is using “Key A” as existing key and that account successfully renewed the public key “Key A” by “Key B” on 1 March 2020, then the validity timeline for keys is below:

From	**To**	**Valid Key(s)**
1 March 2020	14 March 2020	Both “Key A” and “Key B” can be used for login.
15 March 2020	1 March 2022	Only “Key B” can be used for login “Key B” become existing key now.
2 March 2022	~	“Key B” is expired and no key can be used for login. CPs **must** renew their SSH keys before the expiry date. If not, CPs are required to follow Section 5 to re-register the public key with HKEX

6.2 Expiry Notification

When there is a SSH key to be expired in coming 14 days, a report named "SSHKeyExpireWarning_yyyymmdd.txt" will be generated under /KEY_MANAGEMENT folder. CPs should check the /KEY_MANAGEMENT folder regularly and follow the renewal procedure in Section 6 to renew their SSH key before the SSH key expire.

Since the to-be-expired SSH key and the renewed key will co-exist and continue to be valid for 14 days, the expiry report will be generated daily until the to-be-expired SSH key is expired and removed by system. CPs can ignore the expiry report if they has successfully renewed the SSH key.

6.3 Frequent Upload Control

Each SFTP user account will be restricted to upload maximum of five keys (regardless of the upload results) within one hour. The upload feature will be blocked (unable to upload and "Permission Denied" will be shown when attempt to upload) once five keys has been uploaded within one hour or reach 120 daily upload limit. The upload feature will be automatically unblock after one hour from blocked.

For example, if a SFTP user account has uploaded 5th key at 12:45:10, the upload feature will be blocked at 12:45:10 then unblock at 13:45:10 automatically.

7 Network Configuration

The SFTP facility is only accessible from the Securities and Derivatives Network/2 (SDNet/2) or HKEX Service Network (HSN).

CPs can register two designated SFTP client workstations for report retrieval. Follow Section 5 above, CPs should submit the IP addresses of their designated SFTP client workstations to HKEX for registration.

Upon registration of public keys and IP addresses, CPs can access HKEX SFTP facility with the assigned user accounts via either one of the registered SFTP client workstations.

IP addresses of the SFTP client workstations must be within the same subnet (first 3 octets) of SDNet/2 or HSN.

7.1 Connectivity of HKEX SFTP Facility

IP addresses of HKEX SFTP facility are as follows:

HKEX SFTP Facility at primary data center	**HKEX SFTP Facility at secondary data center**
10.151.14.121 port 10022 10.151.14.122 port 10022	10.152.14.121 port 10022 10.152.14.122 port 10022