HKSCC Internet Report Access Platform (iRAP)

Technical Guide

Version:	0.1
Date:	Feb 2020

Modification History

Version	Date	Modified By	Synopsis
0.1	Feb 2020	HKSCC	First Draft

Table of Contents

1 Overview

1.1 Background

This document serves as a technical reference guide for HKSCC's Master SPSA Holders to retrieve the Day-begin Sellable Balance Reports through Internet Report Access Platform (iRAP) via an Secure File Transfer Protocol (SFTP) facility provided by HKSCC.

It covers the following areas of the iRAP:

- Technical Infrastructure
- Access to iRAP via SFTP Facility
- Operation of iRAP
- Registration of iRAP SFTP User Account
- Network Configuration
- Report Details
- Important Notes

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

All Master SPSA Holders are required to ensure that the SFTP client (in-house developed or third-party software) installed in their iRAP client workstations for report / file retrieval must adhere to the above standard.

2.2 Primary SFTP Facilities

The SFTP facility is set up at HKSCC's primary data center. Under normal situation, the primary SFTP facility is in active mode. For contingency situation where the primary SFTP facility becomes unavailable, HKSCC will notify Master SPSA Holders to retrieve the report by other means.

3 Access to iRAP Via SFTP Facility

3.1 User Accounts

Each Master SPSA Holder will be issued with two iRAP SFTP user accounts by HKSCC for access to the iRAP.

The two iRAP SFTP user accounts are in the following format:

- F*xxxxx*001
- F*xxxxx*002

Where <F*xxxxx*> is the Master SPSA Holder ID. For example, iRAP SFTP user accounts F12345001 and F12345002 would be assigned to Master SPSA Holder with ID F12345.

After registration (refer to Section 5 for registration details), Master SPSA Holders may use either one of the assigned iRAP SFTP user accounts together with the respective SSH private key to login to the iRAP for retrieval of reports/ files. Upon receipt of the assigned user accounts, Master SPSA Holders are recommended to verify and ensure both of their assigned SFTP user accounts can access the iRAP.

3.2 Secure Shell (SSH) Keys

SFTP facility adopts Secure Shell (SSH) public-key authentication. For each iRAP SFTP user account, Master SPSA Holders need to generate a pair of SSH private and public keys, as well as a SSH key fingerprint, and register the SSH public key together with the SSH key fingerprint with HKSCC.

3.2.1 SSH Public Keys

HKSCC accepts RSA 2048-bit SSH 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 SSH public key should be saved in a separate file with the following naming convention and sent to HKSCC via email for registration:

- F*xxxxx*001.pub (public key for iRAP SFTP user account F*xxxxx*001)

- F*xxxxx*002.pub (public key for iRAP SFTP user account F*xxxxx*002)

Where < F*xxxxx* > is the Master SPSA Holder ID.

3.2.2 SSH Key Fingerprints

SSH key fingerprints are MD5 message 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 HKSCC via email for registration:

- F*xxxxx*001.fpt (SSH key fingerprint for iRAP SFTP user account F*xxxxx*001)
- F*xxxxx*002.fpt (SSH key fingerprint for iRAP SFTP user account F*xxxxx*002)

SSH public keys and SSH key fingerprints together with the IP addresses (refer to Section 6 for network configuration) of their designated iRAP SFTP client workstations for accessing iRAP should be submitted to HKSCC through email for registration. See Section 5 for details.

Master SPSA Holders SHOULD NOT submit their SSH private keys to HKSCC for registration.

3.3 Pretty Good Privacy (PGP) Keys

The SFTP facility of iRAP performs Pretty Good Privacy (PGP) public-key file encryption for the Day-begin Sellable Balance Reports per Master SPSA Holder ID (e.g. Fxxxxx). All reports distributable to the same Master SPSA Holder will be encrypted with the same PGP public key. Master SPSA Holders need to generate a pair of PGP private and public keys, as well as a PGP key fingerprint, and register the PGP public key and the PGP key fingerprint with HKSCC.

3.3.1 PGP Public Keys

HKSCC accepts RSA 2048-bit public keys in PGP format.

For example:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBF3pxlEBCACosTj0mKxNad7QI87MmOz8KZLhyGJ3uoR1gehoQHY7kFfbw75z
ylkTKPTSVQbkFz9OR4Ppy5PLcyOBVaiCe+fNdG1YonoraFkNcsLFuxIT/t5VHIgV
+M4x7+fPYCG4j+gGUzpUshbW64gpb9nw7VRWjBo357qUQC9myy0tQ34DhpUreKry
pchO+l3oKtle1KFM9qFobGGn0C139hKRd6mUFlupTKwYMdmtmwJGCv5ld+fDnrkS
VuigAXya3AVRTUn6aGgYdO6BBHcA3MO+rVvBivevo1YdGQkjgqoPQ9CV0UWIiDvE
1HMRt+WrjAqyRSmhuOzA2Rvd0qcYggwN5NudABEBAAG0JUY0MDAwMl9QR1BfMDEg
KFBHUCBrZXkgZm9yIEY0MDAwMl8wMSmJAU4EEwEIADgWIQSWtBYvcpsouhVbTqNW
KG31phIdowUCXenGUQIbIwULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRBWKG31
```

```
phIdo2BbCACQtzTQHlEfkOiMeW4KErLNx7Yk4jb0Q6JACDQKIqOLBtFMYwSehgCi
6vzwUUpd76S9OlBehBckw98ldGbNsS3v1ZwGMtxFjryY62CFMh3HE/gfnHakowuH
YIqTPr6ztolNDdznoDgeJgxMepGqwvmmNgLf7+FyYxYfNWXwHif+54ByJUQAj5wv
oV3q1yuiqU1xIzprnJQebf1S/xbnXNS5+i6mmAl5W9JSaGtigsPGvaTIN1VxjfTg
NXhS2Jqr27eqRrxHJq0MTBgkpKwztUmR1JHjgCDxXci5I0o8nSWrnCdUF1zr8Nqq
77a2W4aOuba5JKrxUDd2crYAkqIHBMLuuQENBF3pxlEBCADJRH2A05CTKVbaKod9
+K0ze4O98S/wCoEayODJNUV0xQL4fsuW4XQUykHR7JUnpGNdaGIIrSz46p5mVY7U
+LksZ+UvyNzdUq1l+JMmDn45YfRTU8pCV6AsvvfWsu44FMKlwYsoRRAR5MTByIB8
Jm0PNzMu56hMz9Zp9flrbzUgtIkFh7BHfQcvZ7XlOLQROlCRYZQTS8k8L50Tt3tn
Kn8ET9qzDnBWU/DvDTk9AM8tvW92cM5Tbd5aWKAIn5TPoNZhWK5GwKre+v4ojiqm
EKDXAIBmHSTh0DlFQKUtz8TVEtKmm+L3BeRBt10qRyd/ySoEY28v9vyee0DxFiL6
CDb7ABEBAAGJATYEGAEIACAWIQSWtBYvcpsouhVbTqNWKG31phIdowUCXenGUQIb
DAAKCRBWKG31phIdo4VeB/44YfE+Nymn3yE3ILldytBDszZiQx8iRsUJrXbOnbcW
3VMkf8aIiUxi/XtAYcx2Kli2HxHfL7dAhX4u9W7BI3AVYYNPe6xsHyf/trPIPDRS
hv0gidhOi6vQyBzINWFZLM/yiNLrFugSp+7oBGwH0V5VhG1a5aoXk4veTgqDK4vo
0UoEPW6kRwqIlzVl4dy7VzplnS/W2WgSPpRpsmoTzwxeUrWMIwg6FhPgOvywYdbH
WlyWVvJ93qKAo0JaeW14yawV+goGGDLoPutIjrRC8LoAfQYe4T63xTcGsolyoYkb
qvYDebvF8gPBb4GNa2uXT198e4Jc/kxHwgjzuLqvGVUn
=6IOV
-----END PGP PUBLIC KEY BLOCK-----
```

The PGP public key should be saved in a separate file with the following naming convention and sent to HKSCC via email for registration:

- F*xxxxx*.asc (PGP public key for Master SPSA Holder ID F*xxxxx*)

Where < F*xxxxx* > is the Master SPSA Holder ID.

3.3.2 PGP Key Fingerprints

PGP key fingerprints are message digests of public keys in the format of 10 octets printed as hexadecimal with uppercase letters and separated by space.

For example:

"4CA8 AE06 6377 E19C 9DC3 3082 33A4 7AC6 4939 226A"

The PGP key fingerprint should be saved in a separate (text) file with the following naming convention and sent to HKSCC via email for registration:

- F*xxxxx*.fpt (PGP key fingerprint for Master SPSA Holder ID F*xxxxx*)

PGP public key and PGP key fingerprint should be submitted to HKSCC through email for registration. See Section 5 for details.

Master SPSA Holders SHOULD NOT submit their PGP private key to HKSCC for registration.

4 Operation of iRAP

4.1 Operation Hours and Time Schedule

Operation hours of iRAP are from 07:00 - 24:00 on each business day.

All Day-begin Sellable Balance Reports will be kept on the platform available for retrieval for 10 calendar days after their generation. Master SPSA Holders should retrieve and safe keep their reports/ files in a timely manner.

4.2 Folder Structure

Each iRAP SFTP user account has four accessible folders in iRAP, as follows:

Folder	Usage
COMMON	Reports/ files applicable to all Master SPSA Holders
INBOX	Reports/ files applicable to designated Master SPSA Holder <Fxxxxx> only
KEY_MANAGEMENT	For submission of SSH public keys for renewal by Master SPSA Holder per iRAP SFTP user account, e.g.<Fxxxxx001>
PGP_KEY_MANAGEMENT	For submission of PGP public keys for renewal by Master SPSA Holder per Master SPSA Holder ID <Fxxxxx>

iRAP SFTP user accounts assigned to the same Master SPSA Holder (i.e. account names start with the same Master SPSA Holder ID) can access the same set of folders. Thus, both iRAP SFTP user accounts (<Fxxxxx001> and <Fxxxxx002>) can retrieve same set of reports/ files generated by HKSCC from the /INBOX folder.

The /KEY_MANAGEMENT folder is for submitting SSH public keys for renewal, each iRAP SFTP user account (e.g. Fxxxxx001) will be assigned with an individual /KEY_MANAGEMENT folder and it cannot be shared with other iRAP SFTP user account.

For /PGP_KEY_MANAGEMENT folder, Master SPSA Holder is able to upload its new PGP public key (signed by original PGP private key) for self-service key renewal per Master SPSA Holder ID (e.g. Fxxxxx) using any of the iRAP SFTP user accounts.

4.3 Frequent Sign-on Control

Each iRAP 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 will be automatically unlocked at every 5 minutes interval.

For example, if an iRAP SFTP user account has been 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 iRAP SFTP User Account

5.1 Initial Registration

To register for iRAP SFTP user accounts, Master SPSA Holders should generate a pair of SSH public and private keys with SSH key fingerprint per account and a pair of PGP public and private keys with PGP key fingerprint. They should then submit their SSH public keys, SSH key fingerprints, PGP public key, PGP key fingerprint and IP addresses of the designated SFTP client workstations to HKSCC in a single zip file (see sample file below), together with a scanned copy of the "Registration Form for Internet Report Access Platform (iRAP)" (add link to the form) via email.

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

- Fxxxxx.zip (where < Fxxxxx > is the Master SPSA Holder ID) containing
    a. SSH public key files (Fxxxxx001.pub; Fxxxxx002.pub),
    b. SSH key fingerprint files (Fxxxxx001.fpt; Fxxxxx002.fpt),
    c. PGP public key file (Fxxxxx.asc),
    d. PGP key fingerprint file (Fxxxxx.fpt) and
    e. Excel template filled with the IP addresses of 2 iRAP client workstations and file names of public keys

A sample zip file can be found on the registration form. Master SPSA Holder should attach the above mentioned zip file with a completed registration form and submit to HKSCC via email, following the procedures as specified in the form.

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

DO NOT ATTACH SSH and PGP private keys in the zip file. Master SPSA Holders should keep their private keys confidential to prevent unauthorized usage.

5.2 Self-service Renewal of Public Keys

Master SPSA Holders are required and recommended to renew their SSH and PGP public keys respectively at least every two years. Master SPSA Holders should also re-register their keys with HKSCC immediately if the corresponding private keys are being compromised. See Section 5.3.

5.2.1 SSH Public Keys (Self-service Renewal)

Renewal of SSH Public Key

Master SPSA Holders **must** renew their SSH public keys every two years.

After generation of the new SSH public keys, Master SPSA Holders should re-register their new SSH public keys with HKSCC by submitting them to the /KEY_MANAGEMENT folder. After submission, a result file will be generated and available for retrieval in the /KEY_MANAGEMENT

folder.

Master SPSA Holders should take the following steps to perform self-service SSH public key renewal:

1. Login iRAP SFTP user account (e.g. FXXXXX001) via SFTP client software.
2. Locate /KEY_MANAGEMENT folder.
3. Upload the new SSH public key into /KEY_MANAGEMENT folder and it will be automatically imported with validity of 730 days for the account logged in. /KEY_MANAGEMENT folder is for upload only, modification and deletion is not allowed.
4. Renew SSH public key for each iRAP SFTP user account separately, i.e. log in FXXXXX001 to renew FXXXXX001's SSH public key and log in FXXXXX002 to renew FXXXXX002's SSH public key.

Results:

- Result file will be generated under /KEY_MANAGEMENT folder after the key has been imported.
- The result file will be named as Result.yyyymmdd.hhmmss.**success**.txt or Result.yyyymmdd.hhmmss.**failed**.txt.
- The result file will specify the file name of the uploaded SSH public key, import date, file size and import result.
- Error reason will be provided if import is failed.
- New SSH public key will be effective immediately if it is imported successfully. The old SSH public key will be expired after 14 calendar days since the new SSH public key has been uploaded.

5.2.2 PGP Public Key (Self-service Renewal)

Renewal of PGP Public Key

Master SPSA Holders are recommended to renew their PGP public keys every 2 years.

After generation of the new PGP public key, Master SPSA Holder should re-register its new PGP public key with HKSCC by submitting it to the /PGP_KEY_MANAGEMENT folder. After submission, a result file will be generated and available for retrieval in the /PGP_KEY_MANAGEMENT folder.

Master SPSA Holder should take the following steps to perform self-service PGP key renewal:

1. Create the new PGP public and private keys.
2. Sign the new PGP public key using the existing PGP private key.
3. Log in iRAP via SFTP client software using any of the iRAP SFTP user accounts (e.g. FXXXXX001 or FXXXXX002).
4. Locate /PGP_KEY_MANAGEMENT folder.
5. Upload new signed PGP public key into /PGP_KEY_MANAGEMENT folder and it will be automatically imported to the account logged in and for the accounts under the same Master SPSA ID (e.g. FXXXXX).

Results:

- Result file will be generated under /PGP_KEY_MANAGEMENT after the key has been imported.
- The result file will be named as Result.yyyymmdd.hhmmss.**success**.txt or Result.yyyymmdd.hhmmss.**failed**.txt.
- The result file will specify the file name of the uploaded PGP public key, import date, file size and import result.
- Error reason will be provided if import is failed.
- New PGP public key will be effective immediately for file encryption if it is imported successfully. Master SPSA Holders are required to use the new PGP private key to decrypt the new reports generated after successful renewal.

5.3 Re-registration of Public Keys (Only when private keys are being compromised)

In case any of the SSH or PGP private keys is lost or damaged, Master SPSA Holders should generate a new set of keys, register and submit the new public keys, key fingerprints and the completed registration form via email (following the procedures specified in the form) to HKSCC for re-registration.

6 Network Configuration

The iRAP is accessible from Internet. Master SPSA Holders can register two designated SFTP client workstations for report retrieval. Following Section 5 above, Master SPSA Holders should submit the IP addresses of their designated SFTP client workstations to HKSCC for registration.

Upon registration of SSH public keys with fingerprints and IP addresses, Master SPSA Holders can access HKSCC SFTP facility with the assigned iRAP SFTP user accounts via either one of the registered SFTP client workstations.

IP addresses of the iRAP SFTP client workstations must be **public** IP addresses. Master SPSA Holders should provide the public IP addresses offered by their Internet Service Provider for access to the internet.

6.1 Connectivity of iRAP

IP address of HKSCC iRAP is as follows:

HKSCC iRAP Facility
iRAP.hkex.com.hk Port 10022

6.2 Authenticity of iRAP

The Master SPSA Holder can verify the validity of HKSCC's sFTP server (iRAP.HKEX.COM.HK) by checking the server SSH host key fingerprint. The fingerprint should match the following value according to the fingerprint algorithm and format supported by their sFTP client.

Algorithm (Format)	Fingerprint
SHA-256 (Hex)	`9b:7c:94:86:dc:5b:11:ba:24:4d:94:bf:09:dd:6d:05:41:03:de:b5:ad:37:b6:34:56:6f:61:e5:6b:dc:fc:e6`
SHA-256 (Base64)	`m3yUhtxbEbokTZS/Cd1tBUED3rWtN7Y0Vm9h5Wvc/OY=`
MD5 (Hex)	`35:60:2c:ff:a4:c0:0b:c5:50:57:52:4a:18:a8:18:1a`

7 Report Details

7.1 Day-begin Master SPSA Sellable Balance Report

The Day-begin Master SPSA Sellable Balance Report is in a Comma-Separated Values format (.csv), found in each iRAP SFTP user account's INBOX folder. It contains the day-begin aggregate sellable balance of the Master SPSA ID based on its underlying SPSA IDs.

The file name of the .csv file follows the naming convention below:

"G29_<FM-ID>_<MasterSPSA-ID>_<TradingDate>.csv"

The table below shows the fields contained in the report of different field lengths:

Field Name	Field Length (Max)	Remark
Master SPSA ID	6	Numeric value
Market Code	4	"ASHR" for Shanghai or "ASZR" for Shenzhen
CSC Stock Code	6	Numeric value
CCASS Stock Code	5	Numeric value
Master SPSA ID Sellable Balance	18	Numeric value
SPSA ID	6	Numeric value
SPSA ID Sellable Balance	15	Numeric value

The following shows a sample layout of the report:

```
Master SPSA ID,Market Code,CSC Stock Code,CCASS Stock Code,Master SPSA ID
Sellable Balance,SPSA ID,SPSA ID Sellable Balance
123456,XXXX,123456,12345,1234567890123456789,123456,123456789012345
123456,XXXX,123456,12345,1234567890123456789,123456,123456789012345
123456,XXXX,123456,12345,1234567890123456789,123456,123456789012345
```

For example, this would be a report file for the Master SPSA “987987”:

```
Master SPSA ID,Market Code,CSC Stock Code,CCASS Stock Code,Master SPSA ID
Sellable Balance,SPSA ID,SPSA ID Sellable Balance
987987,ASZR,1,70001,123456,100001,100000
987987,ASZR,1,70001,123456,100002,20000
987987,ASZR,1,70001,123456,100003,3000
987987,ASZR,1,70001,123456,100004,400
987987,ASZR,1,70001,123456,100005,50
987987,ASZR,1,70001,123456,100006,6
987987,ASZR,8,70008,111,100001,100
987987,ASZR,8,70008,111,100002,10
987987,ASZR,8,70008,111,100003,1
987987,ASZR,46,70046,22220,100003,20000
987987,ASZR,46,70046,22220,100004,2000
987987,ASZR,46,70046,22220,100005,200
987987,ASZR,46,70046,22220,100006,20
987987,ASHR,600002,90002,333330,100001,300000
987987,ASHR,600002,90002,333330,100002,30000
987987,ASHR,600002,90002,333330,100003,3000
987987,ASHR,600002,90002,333330,100004,300
987987,ASHR,600002,90002,333330,100005,30
987987,ASHR,600008,90008,444400,100003,400000
987987,ASHR,600008,90008,444400,100004,40000
987987,ASHR,600008,90008,444400,100005,4000
987987,ASHR,600008,90008,444400,100006,400
(This report is for reference only.  HKEX and/or its subsidiaries do not
guarantee its accuracy and reliability and accept no liability (whether in
tort or contract or otherwise) for any loss or damage arising from any
inaccuracy or omission or from any decision, action or non-action based on
or in reliance upon information contained in this report.)
<End of Report>
```

8 Important Notes

8.1 Usage Guidelines

1. Master SPSA Holders are recommended to poll and retrieve reports/ files from iRAP ONLY when needed e.g. around the time when the reports/ files being available. In addition, any intensive polling should be avoided.

2. Usage management

   For efficient use of network bandwidth and to shorten download time, Master SPSA Holders are advised NOT to use commands such as “mget *.*” when downloading files, otherwise all files retained in the folder (i.e. all reports/ files for past 10 calendar days), will be downloaded. Master SPSA Holders are recommended to only retrieve those reports/ files that have not been downloaded before.

3. Zip file format

   Master SPSA Holders should note that the zip files downloaded from iRAP are encrypted in PGP format. It is necessary to decrypt the files using their own PGP private key.