



Report Access Platform (RAP)

Technical Guide

Version:	1.0
Date:	July 2026

Modification History

Version	Date	Synopsis
1.0	Jul 2026	Initial Publication. Consolidation of technical guides from different clearing houses, update of upload controls and inclusion of specific guidelines for HKSCC Corporate Action Instructions.

Disclaimer

HKEX and/or its subsidiaries endeavour to ensure the accuracy and reliability of the information provided, but 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 document.

No part of this document may be copied, distributed, transmitted, transcribed, stored in a retrieval system, translated into any human or computer language, or disclosed to third parties without written permission from HKEX.

HKEX reserves the right to amend any details in this document at any time, without notice.

Audience and Applicability

This guide is intended for external parties that require access to the Report Access Platform (RAP) for the retrieval and, where applicable, submission or exchange of files across HKEX clearing house services.

The primary audience includes, but is not limited to:

- Participants of HKSCC, HKCC and SEOCH;
- OTC Clear Clearing Members, Clearing Brokers and Sponsored Settlement Members;
- Designated Banks of HKSCC;
- Share Registrars;
- The Hong Kong Inland Revenue Department; and

System vendors and service providers acting on behalf of the above parties may also refer to this guide.

Abbreviations

CA	Corporate Action
CCASS	Central Clearing and Settlement System
CCMS	Clearing and Collateral Management System
CRP	Corporate Representative/ Proxy
DCASS	Derivatives Clearing and Settlement System
EOD	End of Day
FINI	Fast Interface for New Issuance
HKCC	HKFE Clearing Corporation Limited
HKEX	Hong Kong Exchanges and Clearing Limited
HKSCC	Hong Kong Securities Clearing Company Limited
HSN	HKEX Service Network
INT	Intraday
IP	Internet Protocol
IRD	The Hong Kong Inland Revenue Department
MQ	Message Queue
NAT	Network Address Translation
OASIS	OTC Account Services Information System
OCASS	OTC Clearing and Settlement System
OTC Clear	OTC Clearing Hong Kong Limited
RAP	Report Access Platform
RPF	Risk Parameter File
SDNet/2	Securities and Derivatives Network / 2
SEOCH	The SEHK Options Clearing House Limited
SFTP	Secure File Transfer Protocol
SOD	Start of Day
SSH	Secure Shell
SSM	Sponsored Settlement Member
SUB	Subscription
TCP/IP	Transmission Control Protocol / Internet Protocol
USM	Uncertificated Securities Market
VaR	VaR Platform

Table of Contents

Part I – Introduction	9
1. PURPOSE OF THIS GUIDE	9
2. DOCUMENT STRUCTURE AND HOW TO USE THIS GUIDE	9
Part II – General RAP Technical and Operational Framework.....	10
3. SERVICE OVERVIEW	10
3.1. <i>Overview of File Retrieval/ Submission Services</i>	<i>10</i>
3.2. <i>Common Operating Principles.....</i>	<i>10</i>
3.3. <i>Primary and Secondary / Backup Facility.....</i>	<i>11</i>
4. TECHNICAL STANDARDS.....	12
4.1. <i>Supported SFTP / SSH Standards.....</i>	<i>12</i>
4.2. <i>Authentication Standards</i>	<i>12</i>
4.3. <i>Client Software / Tooling Considerations</i>	<i>12</i>
5. USER ACCOUNT REGISTRATION AND KEY RENEWAL.....	13
5.1. <i>User Account and Credential Protection Principles</i>	<i>13</i>
5.2. <i>Secure Shell Key.....</i>	<i>13</i>
5.3. <i>Public Key Format and Fingerprint Requirements</i>	<i>14</i>
5.4. <i>Key Expiry Monitoring.....</i>	<i>15</i>
5.5. <i>Key Renewal.....</i>	<i>15</i>
5.6. <i>Re-registration Due to Compromise.....</i>	<i>17</i>
6. OPERATIONAL USAGE STANDARDS.....	18
6.1. <i>Logon / Logoff Expectations</i>	<i>18</i>
6.2. <i>Download Control.....</i>	<i>18</i>
6.3. <i>Upload Control</i>	<i>19</i>
6.4. <i>Prohibited / Discouraged Commands and Behaviours</i>	<i>20</i>
6.5. <i>Local Storage and Retention by Participants / Members.....</i>	<i>21</i>
7. CONNECTIVITY AND NETWORK CONTROL PRINCIPLES.....	22
7.1. <i>Network Access via SDNet/2 or HSN.....</i>	<i>22</i>
Part III – Use Case-Specific Annexes.....	23
ANNEX A – HKSCC CCASS AND VAR REPORTS-SPECIFIC GUIDELINES	23
A1. <i>Purpose and Applicability</i>	<i>23</i>
A2. <i>RAP User Account Registration / Maintenance</i>	<i>23</i>
A3. <i>RAP User Account Model</i>	<i>23</i>
A4. <i>Public Key Naming Convention and Submission Requirements</i>	<i>24</i>
A5. <i>Service Hours and Availability Window</i>	<i>25</i>
A6. <i>Folder Structure</i>	<i>25</i>
A7. <i>Connectivity Details</i>	<i>27</i>
A8. <i>Recommendations.....</i>	<i>27</i>
A9. <i>Enquiries and Support.....</i>	<i>31</i>
ANNEX B – HKSCC CORPORATE ACTION INSTRUCTIONS (FOR CCASS PARTICIPANTS) -SPECIFIC GUIDELINES.....	32
B1. <i>Purpose and Applicability</i>	<i>32</i>
B2. <i>RAP User Account Registration / Maintenance</i>	<i>32</i>
B3. <i>RAP User Account Model</i>	<i>32</i>
B4. <i>Public Key Naming Convention and Submission Requirements</i>	<i>32</i>
B5. <i>Service Hours and Availability Window</i>	<i>33</i>
B6. <i>Folder Structure</i>	<i>33</i>
B7. <i>Detailed File Matrix – Submission</i>	<i>34</i>

<i>B8. File Submission and Limits</i>	36
<i>B9. Connectivity Details</i>	38
<i>B10. Enquiries and Support</i>	39
ANNEX C – HKSCC DEPOSITORY, NOMINEE AND ISSUER SERVICES (FOR SHARE REGISTRARS)-	
SPECIFIC GUIDELINES	40
<i>C1. Purpose and Applicability</i>	40
<i>C2. RAP User Account Registration / Maintenance</i>	40
<i>C3. RAP User Account Model</i>	40
<i>C4. Public Key Naming Convention and Submission Requirements</i>	40
<i>C5. Service Hours and Availability Window</i>	41
<i>C6. Folder Structure</i>	41
<i>C7. Service-Specific Download Folders</i>	42
<i>C8. Service-Specific Submission Folders</i>	42
<i>C9. Detailed File Matrix – Download</i>	43
<i>C10. Detailed File Matrix – Submission</i>	44
<i>C11. File Submission</i>	47
<i>C12. Connectivity Details</i>	49
<i>C13. Enquiries and Support</i>	50
ANNEX D – HKCC / SECH DCASS AND CCMS REPORTS-SPECIFIC GUIDELINES	51
<i>D1. Purpose and Applicability</i>	51
<i>D2. RAP User Account Registration / Maintenance</i>	51
<i>D3. RAP User Account Model</i>	51
<i>D4. Public Key Naming Convention and Submission Requirements</i>	51
<i>D5. Service Hours and Availability Window</i>	52
<i>D6. Folder Structure</i>	52
<i>D7. Connectivity Details</i>	53
<i>D9. Enquiries and Support</i>	54
ANNEX E – OTC CLEAR OASIS REPORTS AND DIRECT MESSAGING-SPECIFIC GUIDELINES	55
<i>E1. Purpose and Applicability</i>	55
<i>E2. RAP User Account Registration / Maintenance</i>	55
<i>E3. RAP User Account Model</i>	55
<i>E4. Public Key and Submission Requirements</i>	56
<i>E5. Service Hours and Availability Window</i>	56
<i>E6. Folder Structure</i>	56
<i>E7. Reports and File Name Format</i>	58
<i>E8. Connectivity Details</i>	59
<i>E9. Recommendations</i>	60
<i>E10. Enquiries and Support</i>	65
ANNEX F – HKSCC USM SERVICES (FOR IRD)-SPECIFIC GUIDELINES	66
<i>F1. Purpose and Applicability</i>	66
<i>F2. RAP User Account Registration / Maintenance</i>	66
<i>F3. RAP User Account Model</i>	66
<i>F4. Public Key Naming Convention and Submission Requirements</i>	66
<i>F5. Service Hours and Availability Window</i>	67
<i>F6. Folder Structure</i>	67
<i>F7. File Submission</i>	68
<i>F8. Connectivity Details</i>	70
<i>F9. Enquiries and Support</i>	70
Appendices	71
APPENDIX 1 – QUICK REFERENCE MATRIX BY CLEARING HOUSE	71
APPENDIX 2 – REJECTION CODES USED IN SUBMISSION REJECTION FILE	71

APPENDIX 3 – SSH PROTOCOL ALGORITHMS..... 72

Part I – Introduction

1. Purpose of This Guide

This document provides the technical and operational framework for the **Report Access Platform (“RAP”)** and related secure file transfer arrangements covered by this guide. It is intended to serve as a **consolidated guide** for external parties of different clearing houses (“users”) who need to implement, support, use file retrieval and, where applicable, file submission processes across the in-scope clearing house services through RAP.

This guide describes the **common baseline** for technical standards, access control, key management, operational usage, connectivity, monitoring, and contingency handling, while providing the **use case-specific guidelines** set out in the annexes. This structure is intended to provide a consistent overarching framework for users across the covered services, while recognising that each service has distinct characteristics in terms of scope, account model, folder structure and operating guidelines.

This guide should be read together with other applicable HKEX documents, for example, circulars, terminal user guides, installation procedures, technical specifications.

2. Document Structure and How to Use This Guide

This guide is structured to separate common technical and operational requirements from use-case specific guidelines.

- Part I – Introduction describes the **purpose, scope**, and **overall structure** of this guide.
- Part II – **General RAP Technical and Operational Framework** sets out the common requirements that apply across the covered services.
- Part III – Use Case-Specific Annexes provides the **detailed guidelines** applicable to each clearing house or service area as follows:
 - Annex A – HKSCC CCASS and VaR Reports-Specific Guidelines
 - Annex B – HKSCC Corporate Action Instructions (for CCASS Participants)-Specific Guidelines
 - Annex C – HKSCC Depository, Nominee and Issuer Services (for Share Registrars)-Specific Guidelines
 - Annex D – HKCC/ SEOCH DCASS and CCMS Reports-Specific Guidelines
 - Annex E – OTC Clear OASIS Reports and Direct Messaging-Specific Guidelines
 - Annex F – HKSCC USM Services (for IRD)-Specific Guidelines

After reviewing Part I for an overview of the document, users should read the common requirements set out in Part II and then refer to the relevant annex in Part III for the applicable service.

Part II – General RAP Technical and Operational Framework

3. Service Overview

3.1. Overview of File Retrieval/ Submission Services

The services covered by this guide provide secure mechanisms for the retrieval of reports and files and, where applicable, the submission or exchange of files through SFTP-based connectivity.

For HKSCC, RAP is used by **Participants and Designated Banks** to retrieve **CCASS reports** and, where applicable, **VaR reports and Risk Parameter Files**. Participants may also use RAP to submit **Corporate Action Instructions files** to CCASS.

Share Registrars may use RAP to retrieve and/or submit data files relating to **Nominee Services**, including EIPO, Corporate Communications, Corporate Representative / Proxy and USM. The **IRD** may also use RAP to support **stamp duty** processing for USM.

For HKCC/ SEOCH, RAP is used by **Clearing Participants** to retrieve **DCASS, pre-trade risk management and CCMS reports**.

For OTC Clear, the RAP is used by **Clearing Members, Clearing Brokers and Sponsored Settlement Members** to download **OASIS reports**. In the applicable service context, the OTC Clear SFTP framework also supports **Direct Messaging Service**.

Although these services differ in scope and operating model, they share a common foundation based on secure file transfer, controlled user access, key-based authentication and defined operational procedures for file handling.

3.2. Common Operating Principles

The following common operating principles apply to the use of RAP:

- access should only be made through **authorised connectivity arrangements**, using the assigned user account together with the corresponding registered public / private key pair;
- the services should be used solely for the **controlled** retrieval and, where applicable, submission of files required for the relevant business process or processing date;
- **repeated or excessive access, repeated download** of the same files, **concurrent** use of the same account, and the use of **broad wildcard retrieval commands** should be **avoided**;

- where submission functionality is available, files should be prepared, named and submitted in accordance with the applicable service requirements, with **appropriate controls** in place to verify **successful submission** and processing; and
- required files should be **retained in the user's own local environment** for operational use and the RAP should not be relied upon as a substitute for internal storage or record retention.

3.3. Primary and Secondary / Backup Facility

The RAP is designed with resilience arrangements that include a **primary facility** and a **secondary / backup facility**.

The primary facility and the secondary / backup facility are located in separate data centres. Under normal circumstances, users are expected to connect to the primary facility. RAP provides two IP addresses for the primary facility. Both IP addresses of the primary facility are **active** at the same time. **If users encounter a failure when connecting to one of the IP addresses, they should connect to the other IP address.** In the event of a **contingency situation**, RAP connectivity through both IP addresses of the primary facility will be unavailable. **Users will be notified to connect to the secondary / backup facility** to continue operations.

Users should ensure that their network configuration, operational procedures and recovery testing take into account both the primary facility and the applicable secondary / backup facility for the relevant service.

4. Technical Standards

4.1. Supported SFTP / SSH Standards

The RAP uses industry-standard SFTP and supports the following protocols:

Protocol	RFC	Remarks
SFTP	RFC 4251-4254	Secure Shell File Transfer Protocol (Endurance feature is not supported ¹)
SSH Public Key File Format	RFC 4716	SSH2 Public Key File Format Fingerprint: MD5 message-digest

Users are required to ensure that the SFTP software used adheres to the above standards.

4.2. Authentication Standards

The RAP adopts **Secure Shell (SSH) public-key authentication**. For each user account, users should generate an SSH key pair comprising a private key and a public key. The requirements of SSH key are set out in section 5.

4.3. Client Software / Tooling Considerations

Users may use in-house applications or third-party SFTP client software, provided that the selected tool supports the applicable service requirements and adheres to the relevant technical standards.

Where automated tooling is used, users should ensure that the tool is designed to operate in accordance with the applicable service requirements, including correct account usage, key handling, file naming, file location and session control. Appropriate operational controls should also be implemented to monitor file transfer outcomes and detect unsuccessful retrieval or submission attempts.

¹ The endurance feature is not supported by the RAP. Users should ensure that this feature is disabled; otherwise, a "Permission Denied" message may be displayed when files, such as SSH key files, are uploaded.

5. User Account Registration and Key Renewal

5.1. User Account and Credential Protection Principles

Each RAP user account should be used only for the applicable service, use case and business purpose for which it has been assigned. Credentials used for RAP access, including user accounts, private keys and related authentication information, should be protected against unauthorised access, disclosure, alteration or misuse.

Users should ensure that:

- user account including credential and private keys are **accessible only to authorised users, systems or support personnel** on a need-to-use basis;
- each user account is **managed separately**, together with its corresponding SSH key pair and registered workstation;
- user accounts and authentication information are **not shared in an uncontrolled manner** across different teams, systems or service areas;
- **account naming, account format** and any **case-sensitivity requirements** applicable to the relevant service are complied with;
- **private keys are stored securely and are protected** by appropriate logical, procedural and, where applicable, technical controls;
- **private keys are not provided to HKEX**;
- **network configuration, firewall rules and routing settings** support access only from the **authorised environment**; and
- any **backup, transfer or replacement of credentials** is performed in a **controlled and traceable manner**;

The user account registration methods for each service are set out in the relevant annex. Where a service provides more than one user account to a participant, member or related user group, each account should be administered and controlled individually. Users should also ensure that credential protection arrangements remain appropriate throughout the credential lifecycle, including initial setup, ongoing use, renewal, replacement and retirement.

5.2. Secure Shell Key

The SSH key pair is used to authenticate access to the service in a secure manner. The private key should be retained securely by the users, while the public key and, where required, the corresponding fingerprint should be submitted to HKEX for registration or renewal in accordance with the applicable service requirements.

5.3. Public Key Format and Fingerprint Requirements

RAP accepts **RSA between 2048-bit and RSA 4096-bit** public keys in **SSH2 format**. An example is shown below:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: SSH KEY
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIABDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Omleg9e4NnCRleaqqZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKvlgHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GD1B3VVMxHLMxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
```

Each public key should be saved in a **separate file** and should comply with the following requirements:

- the **public key file naming convention** specified to different use cases, if applicable (refer to the relevant annex).
- The file extension must be **“.pub”**
- The file name must **not exceed 128 characters**
- The file name can only contain alphanumeric characters or the following special characters:
 - ‘.’ (dot)
 - ‘-’ (dash)
 - ‘_’ (underscore)
 - ‘ ’ (blank)
 - ‘@’ (ampersand)

Where a public key fingerprint is required, it should correspond exactly to the public key being registered or renewed. **Public key fingerprint is MD5 hash digests of public key** in the format of 16 octets printed as hexadecimal with lowercase letters and separated by colons. An example is shown below:

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

5.4. Key Expiry Monitoring

Users should monitor key validity and expiry. The **public keys are valid for 2 years**.

Where key expiry warnings are provided, users should review them promptly and complete renewal before the relevant key expires.

For RAP services, a **Public Key Expiry Warning File** named `SSHKeyExpireWarning.txt` is generated in the `/key_management/publickey` subfolder when the **current public key is due to expire within 14 days**. The warning is generated based on the user's login time.

The warning file is a fixed-width text file in Windows text format, with each line ending in CR+LF. It contains details of the current public key and, where applicable, the renewed public key, including the creation date, expiration date and fingerprint.

An illustrative example is shown below:

Public Key	Creation Date	Expiration Date	Fingerprint
Current Public Key	2021-02-01	2021-07-15	90:4e:0d:c7:00:37:51:8d:56:5a:a2:d1:93:27:51:2c
Renewed Public Key	2021-07-01	2023-07-01	a2:d1:93:27:51:2c:4e:0d:c7:00:37:51:8d:56:5a:51

After the current public key has expired and has been removed by the system housekeeping job, the warning file will no longer be shown in the folder on the next login.

Users should ensure that any expiry warning, notification or warning file is reviewed without delay and that the corresponding renewal action is completed within the required timeframe to avoid interruption to service access.

5.5. Key Renewal

Users should **renew public keys** within the required timeframe to avoid any interruption to service access.

Users should renew the RAP public key by uploading the new public key to the `/key_management/publickey` subfolder before expiry. After the upload is completed, an **Acknowledgement File** (`.rcvd`) or **Rejection File** (`.rej`) is generated.

The following general notes apply:

- Acknowledgement and Rejection Files are generated on a **per-user-account basis**;
- Acknowledgement and Rejection Files are retained for a maximum of **24 hours** and are subsequently **removed by the end-of-day housekeeping job**;
- if the file name is longer than the system limit of 128 characters, the file will be rejected at SFTP level and no `.rej` file will be generated; and
- public keys submitted through the RAP and other channels are registered in the same

way and carry the same expiry date.

If the upload is successful, the uploaded key will be named “**Renewed Public Key**”. In this case:

- the Renewed Public Key expiry date will be 2 years from the current date;
- the **Current Public Key expiry date** will remain its **original expiry date or 2 weeks from the current date**, whichever is earlier; and
- after the Current Public Key expires, it will be removed and the Renewed Public Key will become the new Current Public Key.

A Renewed Public Key cannot be deleted. However, users may upload another public key to overwrite the existing Renewed Public Key, in which case the corresponding expiry dates will be refreshed. Users may log in using either the Current Public Key or the Renewed Public Key, provided that the relevant key has not expired.

An **Acknowledgement File** (.rcvd) is a **positive acknowledgement** indicating that the uploaded public key file has been accepted. The file name is formatted as <original file name>.<timestamp-HHMMSS>.<seq>.rcvd in the /key_management/publickey subfolder, where .<seq> is optional and appears only when files of the same name are uploaded within the same second and are accepted.

The Acknowledgement File contains a single line showing the fingerprint of the uploaded public key. The fingerprint is presented as an MD5 hash, expressed as 16 octets in lowercase hexadecimal, separated by colons. For example:

```
12:f8:7e:78:61:b4:bf:e2:de:24:15:96:4e:d4:72:53
```

A **Rejection File** (.rej) indicates that the uploaded public key file has been rejected. Users should **review the rejection result promptly, identify the relevant issue and resubmit the corrected public key file** where required.

The Public Key would be rejected if:

- The file name and extension do not meet the requirements listed in section 5.3
- The SSH2 Public Key is not in PEM format
- The PEM header does not have the expected label (i.e. SSH2 PUBLIC KEY)
- The key length is not 2048, 3072 or 4096 bits
- The new Public Key is the same as the current one

- The file does not pass virus scanning

The filename is formatted as <original file name>.<timestamp-HHMMSS>.<seq>.rej in sub-folder /key_management/publickey where .<seq> is optional and appears only when file of same name are uploaded within same second and is accepted.

The .rej file is a text file in window text file format (line ends with CR+LF) in the following format:

#	Field	Type	Size	Remarks
1.	Reject Code	Numeric	5	Reject code
2.	Reject Message	Alphanumeric	255	Reject Message in English

5.6. Re-registration Due to Compromise

Where a private key is suspected to be compromised, lost, disclosed or otherwise rendered untrustworthy, users should stop using the affected credential and complete re-registration in accordance with the applicable service requirements.

6. Operational Usage Standards

6.1. Logon / Logoff Expectations

Users should manage RAP sessions in a controlled manner to prevent concurrent access conflicts and unintended repeated logon attempts.

Users should ensure that:

- **the same user account is not used concurrently** across multiple workstations, servers or sessions;
- Each RAP user account should only be logged in on one designated RAP client workstation at a time;
- **users log off or disconnect promptly** after completing the required retrieval or submission activity;
- connection settings are configured in accordance with the applicable service requirements;
- **repeated logon attempts, unnecessary reconnect activity** or other excessive access behaviour are **avoided**;
- automated processes are designed to control session establishment, file transfer and disconnection in a stable and orderly manner; and
- automated processes use **reasonable retry logic** and do not generate excessive reconnect or repeated polling activity;

Users are advised to **limit login attempts to no more than once per minute**. Login attempts exceeding this recommended frequency may potentially result in a **temporary lockout of the RAP user account for 5 minutes**. The user account will be automatically logged off by the system if the **idle time** reaches **15 minutes**.

6.2. Download Control

Users should retrieve reports or files only for the relevant processing date and should **avoid repeated or excessive downloads** of the same reports, files or messages.

Users should ensure that:

- retrieval jobs are configured to **access the correct date folder or file location for the relevant business date**;
- retrieval is performed for the **intended processing date only** and is **not broadened unnecessarily to other dates**;

- each report, file or message is **downloaded only as required** for the relevant business purpose;
- **each report file should be downloaded only once per day; repeated retrieval of the same report, file or message is avoided** unless and justifiable operationally necessary;
- automated jobs **do not repeatedly download the same content** due to inadequate control logic or missing completion checks; and
- **appropriate retrieval controls** are in place to confirm successful download and prevent unnecessary duplication.

When multiple reports or files are required at the same time, they should be **downloaded within a single RAP logon session**. If the required files are not available, users should also disconnect from RAP and then sign-on again after a brief timeout period of at least 1 minute. Where historical retrieval is required, it should be performed only where there is a clear operational need.

6.3. Upload Control

Users should perform file submission in a **controlled and efficient manner** to ensure stable operation of the RAP service and to **avoid unnecessary system load or processing delays**.

Users should ensure that:

- files are submitted **only when required for the relevant business process** and within the applicable service window;
- **a large number of small files are not submitted at high frequency**. Instead, files should be **batched or consolidated** into appropriately sized files to optimise transfer efficiency and reduce processing overhead;
- submission activities are designed to minimise excessive session establishment, frequent reconnection or repeated upload attempts;
- **each file is submitted only once**, unless a clear operational need for resubmission has been identified;
- automated processes include **appropriate submission control logic to prevent duplicate uploads** caused by retry loops, network interruptions, or similar issues;
- after each submission, users should **verify the outcome by checking the corresponding Acknowledgement File (.rcvd) or Rejection File (.rej)** in the relevant folder;

- in the absence of an Acknowledgement File, or where a Rejection File is generated, users should **review the submission status**, identify the cause and resubmit the corrected file where required;
- during contingency situations (including service disruption or site failover), users should:
 - verify submission status based on the presence of corresponding Acknowledgement Files after site failover (including files acknowledged before failover), and
 - resubmit any files that have not been successfully acknowledged, while ensuring duplicate submissions are avoided through proper reconciliation controls.

To safeguard service stability and ensure fair usage across all users, RAP implements appropriate control measures and safeguards. Details of specific controls for different use cases, where necessary, are set out in the relevant annexes, including but not limited to:

- **rate limiting** or **temporary throttling of file submission** when excessive upload frequency is detected;
- **temporary lockout of user sessions or accounts** maybe applied when abnormal usage patterns are detected (e.g. high-frequency submission, repeated retries or excessive concurrent connections) ;
- **automatic rejection** or blocking of submissions that exceed defined system thresholds or violate operational constraints (e.g. excessive file volume, unsupported behaviour);
- monitoring of submission patterns and system load, with escalation or intervention where activities may adversely impact service performance or other users.

Users are expected to ensure that their systems and operational processes are designed to comply with these controls. Persistent non-compliance may result in further restriction of access.

6.4. Prohibited / Discouraged Commands and Behaviours

Users should **avoid commands, settings or behaviours** that may **create unnecessary load, consume excessive bandwidth or affect usage stability**.

Users should ensure that:

- **broad wildcard commands** such as “mget -r * “ or “get -r **”, **recursive commands or other indiscriminate file-retrieval actions are not used** unless expressly required by the relevant service;
- **unsupported client features or settings** such as endurance, are not enabled where they may affect access, submission or download behaviour;

- prolonged idle sessions, unnecessary repeated reconnect activity or uncontrolled retry loops are avoided; and
- automated tooling is configured to operate in a controlled, predictable and service-compliant manner.

6.5. Local Storage and Retention by Participants / Members

Users should **retrieve and retain required reports and files in their own local environment** in accordance with their operational, control and record-retention requirements.

Users should ensure that:

- downloaded reports and files are saved promptly in an appropriate internal location;
- local storage is used for operational reference, downstream processing and internal retention purposes;
- **RAP is not relied upon as a substitute for internal storage**, archival or record-retention arrangements; and
- appropriate controls are in place to verify that required reports and files have been retrieved and stored successfully.

7. Connectivity and Network Control Principles

7.1. Network Access via SDNet/2 or HSN

Where the relevant service requires access through the Securities and Derivatives Network/2 (SDNet/2) or HKEX Service Network (HSN), users should ensure that the relevant communication line, router and local network setup are provisioned and maintained in accordance with the applicable service requirements. Details of the network access arrangements for each service are set out in the relevant annexes.

Part III – Use Case-Specific Annexes

Annex A – HKSCC CCASS and VaR Reports-Specific Guidelines

A1. Purpose and Applicability

This Annex sets out the use case-specific technical and operational requirements applicable to the retrieval of **CCASS reports**, **VaR reports** and, where subscribed, **Risk Parameter Files** through the RAP. Under this use case, **CCASS Participants** may retrieve CCASS reports, VaR reports and subscribed RPF, while **Designated Banks** may retrieve CCASS reports only.

This Annex should be read together with the common requirements set out in Part II of this guide.

A2. RAP User Account Registration / Maintenance

Requests for RAP user account registration or maintenance should be submitted through **Client Connect** using the **e-Service TechS 8**.

A3. RAP User Account Model

The **maximum number of RAP user accounts** available to CCASS Participants and Designated Banks, together with the applicable **user account naming convention**, are summarised below.

User Type	Maximum Number of RAP User Accounts	Maximum Number of workstations per RAP user accounts	User Account Naming Convention
CCASS Participants	3	4	Format: CXnnnnnn001, where Xnnnnnn is the Participant ID. The user account must be entered in capital letters .
Designated Banks	2	4	Format: CBNKnnnn001, where nnn is the Designated Bank code. The user account must be entered in capital letters .

Users are required to log on using the assigned user account exactly as provided, including case sensitivity.

Each RAP user account should be used together with its corresponding SSH private key.

A4. Public Key Naming Convention and Submission Requirements

For each RAP user account, users should generate a **dedicated SSH key pair** comprising a private key and a corresponding public key.

Each public key must be saved in a separate file and named in accordance with the RAP user account to which it relates. The **public key file, together with its fingerprint and the IP address(es) of the designated RAP client workstation(s)**, should be submitted via Client Connect for registration. Private keys must not be submitted to HKEX.

The required public key file naming convention is as follows:

- **For Participants:**

`CXnnnnnn001.pub` — public key for RAP user account `CXnnnnnn001`, where `Xnnnnnn` represents the Participant ID.

- **For Designated Banks:**

`CBNKnnnn001.pub` — public key for RAP user account `CBNKnnnn001`, where `nnn` represents the Designated Bank code.

Users should ensure that the public key file name matches exactly the corresponding RAP user account.

A5. Service Hours and Availability Window

Report Type	Service Days	Service Hours
CCASS Reports	Monday to Friday (including weekday public holidays)	07:15 – 24:00
	Saturday (except public holidays)	07:15 – 13:00
VaR Reports	Monday to Friday (except public holidays)	07:00 – 24:00

Reports and files are made available for the **past 10 calendar days** from the date of generation. Users should retrieve and save the required reports and files in a timely manner for daily operational use.

A6. Folder Structure

Each RAP user account is granted access to specific folders based on the report type and data subscription applicable to that account. The folder structure and usage principles are described below.

CCASS (including CCMS) Reports

Folder	Description
/download/CCASS_GLOB/yyyymdd /download/CCASS_HKMK/yyyymdd /download/CCASS_MAMK/yyyymdd /download/CCASS_SZMK/yyyymdd	Used for retrieval of CCASS reports and files applicable to all CCASS Participants and Designated Banks (COMMON) as well as reports applicable to a specific Participant (Xnnnnn) or Designated Bank (BNKnnn). Market-specific reports are stored in folders appended with the relevant market code (GLOB, HKMK, MAMK or SZMK).

/download/HKSCC_CCMS_GLOB/yyyymmdd	Applicable only to Cash Clearing Participants for retrieval of CCMS reports and files.
/download/HKSCC_CCMS_HKMK/yyyymmdd	
/download/HKSCC_CCMS_MAMK/yyyymmdd	Includes reports applicable to all related Participants (COMMON) and reports applicable to a specific Participant (Xnnnnn).
/download/HKSCC_CCMS_SZMK/yyyymmdd	Market-specific reports are stored in folders appended with the relevant market code (GLOB, HKMK, MAMK or SZMK).

VaR Platform Reports (applicable to Cash Clearing Participants Only)

Folder	Description
/download/VAR/yyyymmdd	Used for retrieval of VaR reports and files applicable to all related Participants and to specific Participants (Xnnnnn).
/download/RPF_COMMON/yyyymmdd	Available only to specific RAP user with specific subscription. Used for retrieval of Risk Parameter Files (RPF01 – RPF04).
download/RPF_HKEX/yyyymmdd	Available only to specific RAP user with specific subscription. Used for retrieval of Risk Parameter Files (RPF05 – RPF07).

Common Folders

Folder	Description
/key_management/publickey	Used for submission of public keys for key renewal. Each RAP user account is assigned a dedicated key_management folder, which must not be shared with other RAP user accounts.

/submission	<i>Not applicable.</i>
-------------	------------------------

Notes:

- `yyyymmdd` represents the system-generated subfolder for each calendar day. Reports and files generated on a specific day are made available under the corresponding date subfolder.
- Users should retrieve reports and files only from the date subfolder corresponding to the day on which the report or file is generated and made available.
- Access to RPF folders is subscription based. Only Cash Clearing Participants subscribed to the relevant RPF service are permitted to access these folders.

A7. Connectivity Details

RAP is accessible only through the **Securities and Derivatives Network (SDNet/2)** designated for connection to CCASS. Users should refer to the CCASS / VaR Online / RAP Installation Procedures available in Client Connect for the applicable network configuration requirements.

RAP client workstations must be configured with IP addresses that fall within the same SDNet/2 subnet for HKSCC. The applicable subnet ranges are summarised below.

SDNet IP Addresses Subnet	
10.135.0.0/16 10.136.0.0/16	10.176.0.0/14

Users may connect to RAP directly using the applicable IP addresses of the HKSCC RAP.

Primary Data Centre	Secondary / Backup Data Centre
10.243.2.141 port 18801	10.243.66.141 port 18801
10.243.2.142 port 18801	10.243.66.142 port 18801

A8. Recommendations

This section sets out recommended practices for the retrieval of reports, especially the handling of VaR reports and RPF through RAP.

1. Download Performance and Network Impact

The time required to retrieve reports depends on the **size of the files** being downloaded and the available **SDNet bandwidth**. Large file retrieval may occupy SDNet bandwidth for an extended period.

Where RAP shares the same SDNet line with other services, such as CCASS Terminal or VaR Online, Participants should be aware that concurrent retrieval of large files may affect the performance of those services.

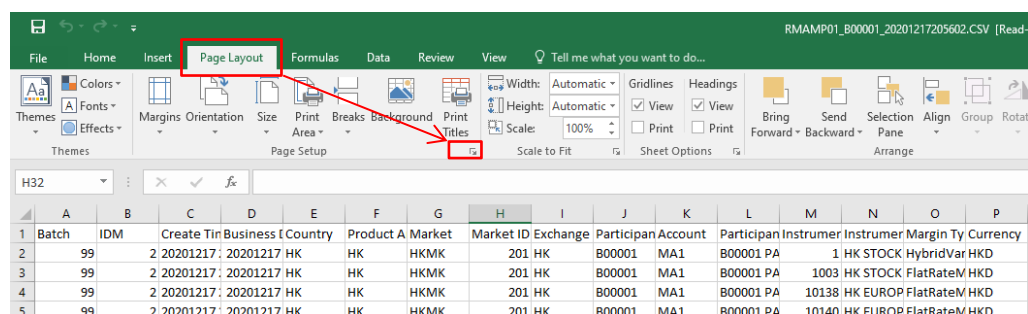
2. VaR reports File Format

VaR reports downloaded from RAP are provided in **CSV format** using the UNIX text convention, where each line is terminated by a Line Feed (LF) character only.

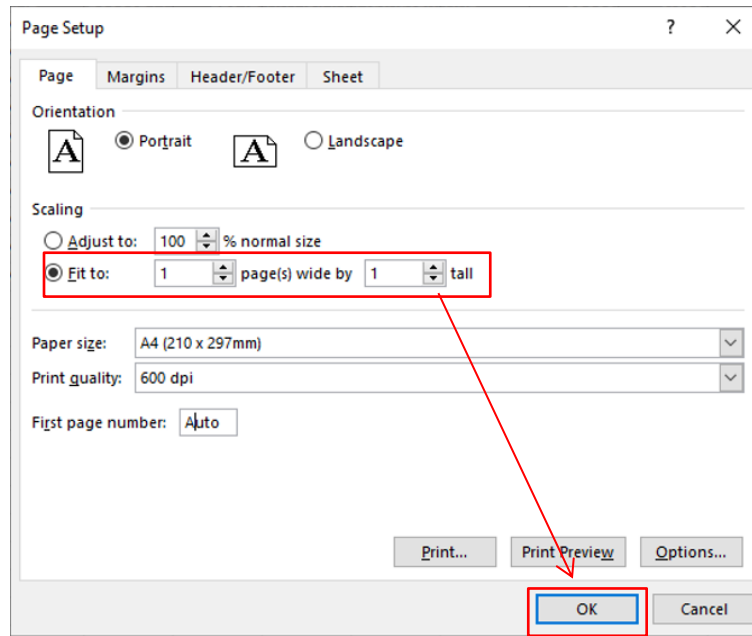
3. Convert VaR reports from csv file to PDF format via Excel

Participants can also convert the CSV files to PDF format by following the steps below:

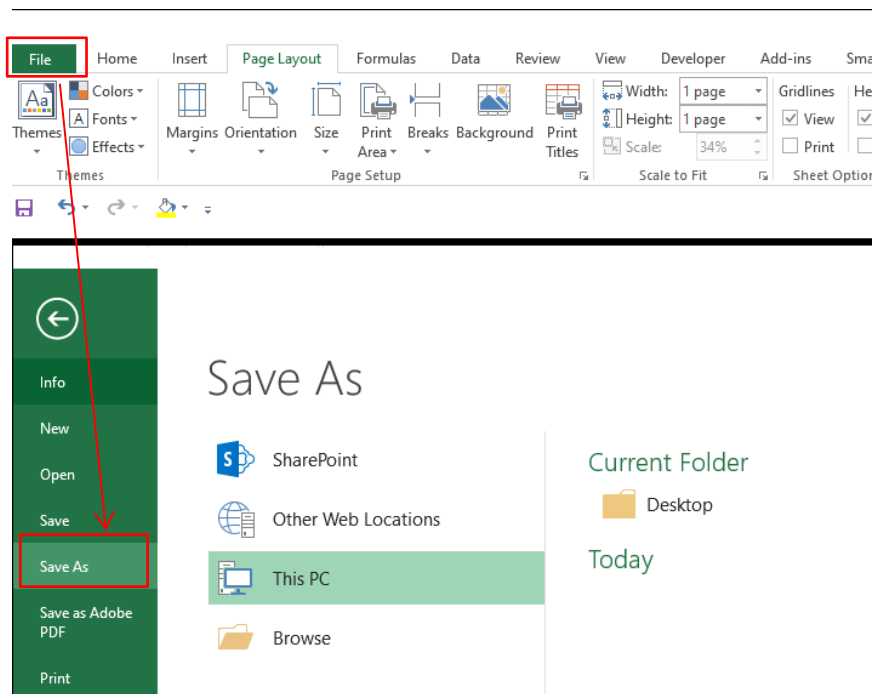
- (i) Open the CSV file in “Excel”
- (ii) Go to “*Page Layout*” tab, and click the “*Page Setup launcher*” at the bottom right corner



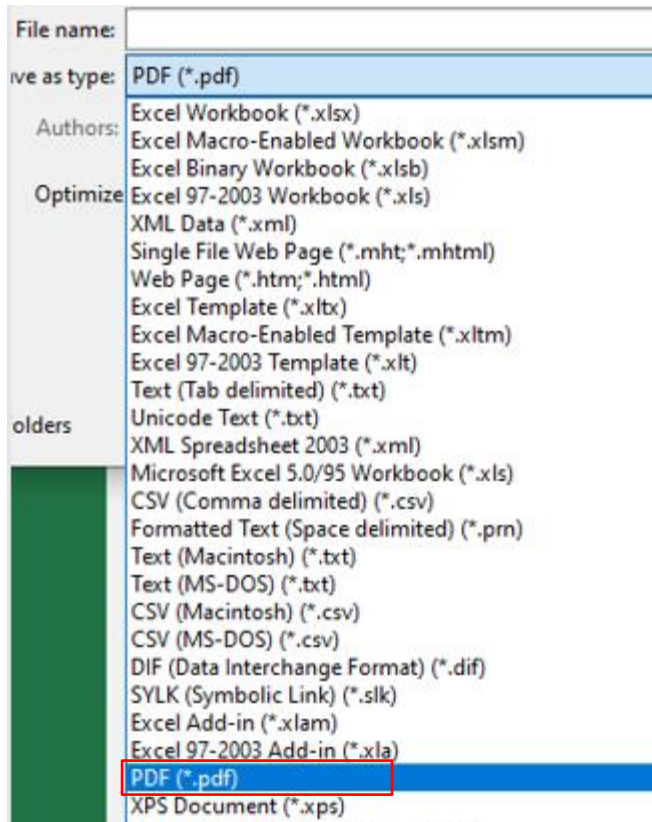
- (iii) In the pop-up window, select the Scaling option: “*Fit to: 1 page(s) wide by 1 tall*”, then click “OK”.



(iv) Go to “File”, click “Save As”, then choose destination location to save the file



(v) Save file as type “PDF (*.pdf)”, and click “Save”.



4. Projected download time for Risk Parameter Files (RPF)

RPF are applicable only to Cash Clearing Participants that have subscribed to the relevant RPF service. RPF files are significantly larger in size than standard reports and may require a longer retrieval time.

The average total RPF size is approximately 1.3GB, and this may increase over time as the number of instruments expands. Users are therefore recommended to ensure that sufficient SDNet bandwidth is available to support timely retrieval. The table below provides an indicative reference for the projected download time of approximately 1.5 GB of data under different SDNet bandwidth configurations.

Bandwidth	Project download time	Bandwidth	Project download time
1M	~4.2 hr	7M	~ 36 min
2M	~2.1 hr	8M	~ 32 min
3M	~1.4 hr	9M	~28 min
4M	~1.1 hr	10M	~ 26 min
5M	~51 min	20M	~ 13 min
6M	~ 42 min	30M	~ 9 min

A9. Enquiries and Support

For any enquiries regarding the use of RAP for retrieving HKSCC CCASS and VaR reports, please contact us through the channels below:

Email: clearingPS@hkex.com.hk / Hotline: 2979 7111

Annex B – HKSCC Corporate Action Instructions (for CCASS Participants) -Specific Guidelines

B1. Purpose and Applicability

This Annex sets out the use case-specific technical and operational requirements applicable to the upload of **Corporate Action Instruction files** to CCASS through the RAP. Under this use case, **CCASS Participants** may upload **Corporate Action Instruction files** to CCASS.

This Annex should be read together with the common requirements set out in Part II of this guide.

B2. RAP User Account Registration / Maintenance

Requests for RAP user account registration or maintenance should be submitted through **Client Connect** using the **e-Service TechS 8**.

B3. RAP User Account Model

The **maximum number of RAP user accounts** available to CCASS Participants together with the applicable **user account naming convention**, are summarised below.

User Type	Maximum Number of RAP User Accounts	Maximum Number of workstations per RAP user accounts	User Account Naming Convention
CCASS Participant	2	4	Format: CXnnnnnn001U, where Xnnnnnn is the Participant ID. The user account must be entered in capital letters .

Users are required to log on using the assigned user account exactly as provided, including case sensitivity.

Each RAP user account should be used together with its corresponding SSH private key.

B4. Public Key Naming Convention and Submission Requirements

For each RAP user account, users should generate a **dedicated SSH key pair** comprising a private key and a corresponding public key.

Each public key must be saved in a separate file and named in accordance with the RAP user account to which it relates. The **public key file, together with its fingerprint and the IP address(es) of the designated RAP client workstation(s)**, should be submitted via Client Connect for registration. Private keys must not be submitted to HKEX.

The required public key file naming convention is as follows:

CXnnnnnn001U.pub — public key for RAP user account CXnnnnnn001U, where Xnnnnnn represents the Participant ID.

Users should ensure that the public key file name matches exactly the corresponding RAP user account.

B5. Service Hours and Availability Window

File Type	Service Days	Service Hours
Voting	Monday to Friday (except public holidays)	07:00 – 19:00
Corporate Representative / Proxy		
Election		
Subscription	Monday to Friday (except public holidays)	07:00 – 19:45 ²
Tender	Monday to Friday (except public holidays)	07:00 – 19:00
	Saturday (except public holidays)	07:00 – 13:00

B6. Folder Structure

Each RAP user account is granted with access to the specific folders based on the submission rights assigned to that account. The folder structure and usage principles are described below.

Corporate Action Instruction files

Folder	Description
/submission/CA_VOTING	For submission of voting instruction files
/submission/CA_CRP	For submission of corporate representative/ proxy instruction files
/submission/CA_ELECTION	For submission of election instruction

² The 19:00 to 19:45 window is strictly reserved for MAMK and SZMK subscription instructions. No other instructions will be processed.

Folder	Description
	files
/submission/CA_SUB	For submission of subscription instruction files
/submission/CA_TENDER	For submission of tender instruction files

Common Folders

Folder	Description
/key_management/publickey	Used for submission of public keys for key renewal. Each RAP user account is assigned a dedicated <code>key_management</code> folder, which must not be shared with other RAP user accounts.
/download	<i>Not applicable.</i>

B7. Detailed File Matrix – Submission

The detailed submission file matrix for this use case is summarized below.

Submission of Voting Instruction File

RAP Folder	/submission/CA_VOTING
Filename Convention	VT_Xnnnnn_<File Indicator>.TXT where Xnnnnn is the participant IFD, <File Indicator> is a unique 4-digits ID specified by users.
File Extension Allowed	TXT
Max File Size	2MB
Auto-append String in Response File Filename	N/A

Submission of Corporate Representative/ Proxy Instruction File

RAP Folder	/submission/CA_CRP
Filename Convention	CR_Xnnnnn_<File Indicator>.TXT where Xnnnnn is the participant ID, <File Indicator> is a unique 4-digits ID specified by users.
File Extension Allowed	TXT
Max File Size	4MB
Auto-append String in Response File Filename	N/A

Submission of Election Instruction File

RAP Folder	/submission/CA_ELECTION
Filename Convention	EL_Xnnnnn_<File Indicator>.TXT where Xnnnnn is the participant ID, <File Indicator> is a unique 4-digits ID specified by users.
File Extension Allowed	TXT
Max File Size	2MB
Auto-append String in Response File Filename	N/A

Submission of Subscription Instruction File

RAP Folder	/submission/CA_SUB
Filename Convention	SU_Xnnnnn_<File Indicator>.TXT where Xnnnnn is the participant ID, <File Indicator> is a unique 4-digits ID specified by users.
File Extension Allowed	TXT
Max File Size	2MB

Auto-append String in Response File Filename	N/A
---	-----

Submission of Tender Instruction File

RAP Folder	/submission/CA_TENDER
Filename Convention	TN_Xnnnnn_<File Indicator>.TXT where Xnnnnn is the participant ID, <File Indicator> is a unique 4-digits ID specified by users.
File Extension Allowed	TXT
Max File Size	2MB
Auto-append String in Response File Filename	N/A

B8. File Submission and Limits

The submission of CA instruction files must be conducted in a controlled and need-based manner. For each /submission sub-folder, users must comply with the limits below or the file submission may be rejected.

RAP Folder	Max. Number of Files Uploaded per Account per Day	Max. Total File size (MB) Uploaded per Account per Day
/submission/CA_VOTING	15	4
/submission/CA_CRP	15	28
/submission/CA_ELECTION	15	2
/submission/CA_SUB	15	2
/submission/CA_TENDER	25	40

Only files successfully accepted by RAP are counted towards these limits. Once the daily limit on the number of files or the total file size has been reached, any further file uploads on the same day will be rejected. CCASS Participants may resume file uploads on the next CCASS working day.

Users submit files to HKEX by **uploading the relevant files to the applicable /submission/<sub-folder> in RAP**. After submission, files are collected and removed from the submission folder immediately, or according to the schedule specified in the corresponding File Interface Specification. Upon completion of processing, the system generates either an Acknowledgement File (`.rcvd`) or a Rejection File (`.rej`).

Each submitted file is subject to the following validation checks:

- the **file name, file extension, file size and submission time** must comply with the rules defined for the relevant submission folder;
- the **Participant ID embedded in the file name** must match the user account.

Users should note the following operational considerations:

- **file renaming functions using RAP rename commands are not supported**; users should ensure that any SFTP client feature that uploads a temporary file name and subsequently renames the file (for example, certain WinSCP settings) is disabled;
- acknowledgement and rejection files are generated on a per RAP user account basis;
- acknowledgement and rejection files are retained for a maximum of **24 hours** and are subsequently **removed by the end-of-day housekeeping job**; and
- if the file name is longer than the system limit of 128 characters, the file will be rejected at SFTP level and no `.rej` file will be generated.

The **Acknowledgement File** (`.rcvd`) generated to the `/submission/<sub-folder>` is a **positive acknowledgement** indicating that the submitted file has been accepted.

The file name is formatted as:

```
<original file name>.<suffix>.<timestamp-HHMMSS>.<seq>.rcvd
```

where the optional sequence number `.<seq>` is appended only when multiple files with the same file name are uploaded from different sessions within same second and are accepted.

For example, if 3 files with the same file name are uploaded within same second and accepted, the `.rcvd` file will be named as:

```
1st file: <original file name>.<suffix>.<timestamp-HHMMSS>.rcvd
```

2nd file: <original file name>.<suffix>.<timestamp-HHMMSS>.1.rcvd

3rd file: <original file name>.<suffix>.<timestamp-HHMMSS>.2.rcvd

The .rcvd file is a fixed-width text file in Windows text file format (CR+LF line ending) and contains the following fields:

#	Field	Type	Size	Remarks
1	Checksum	Alphanumeric	66	SHA-256 checksum of the submitted file for verification
2	Filename	Alphanumeric	128	Filename of the submitted file

The **Rejection File (.rej)** generated to the /submission/<sub-folder> is a **negative acknowledgement** indicating that the submitted file has been rejected.

The filename is formatted as:

<original file name>.<suffix>.<timestamp-HHMMSS>[.seq].rej

For example, if 3 files with the same file name are uploaded within same second and rejected, the .rej file will be named as:

1st file: <original file name>.<suffix>.<timestamp-HHMMSS>.rej

2nd file: <original file name>.<suffix>.<timestamp-HHMMSS>.1.rej

3rd file: <original file name>.<suffix>.<timestamp-HHMMSS>.2.rej

The .rej file is a text file in Windows text file format (CR+LF line ending) and contains the following fields:

#	Field	Type	Size	Remarks
1	Reject Code	Numeric	5	Reject code
2	Reject Message	Alphanumeric	255	Reject Message in English

B9. Connectivity Details

RAP is accessible only through the **Securities and Derivatives Network (SDNet/2)** designated for connection to CCASS. Users should refer to the CCASS / VaR Online / RAP Installation Procedures available in Client Connect for the applicable network configuration requirements.

RAP client workstations must be configured with IP addresses that fall within the same SDNet/2 subnet for HKSCC. The applicable subnet ranges are summarised below.

SDNet IP Addresses Subnet	
10.135.0.0/16 10.136.0.0/16	10.176.0.0/14

Users may connect to RAP directly using the applicable IP addresses of the HKSCC RAP.

Primary Data Centre	Secondary / Backup Data Centre
10.243.2.151 port 18801	10.243.66.151 port 18801
10.243.2.152 port 18801	10.243.66.152 port 18801

B10. Enquiries and Support

For any enquiries regarding the use of RAP for submitting CA instructions, please contact us through the channels below:

Email: clearingPS@hkex.com.hk / Hotline: 2979 7111

Annex C – HKSCC Depository, Nominee and Issuer Services (for Share Registrars)-Specific Guidelines

C1. Purpose and Applicability

This Annex sets out the use cases, specific technical and operational requirements applicable to the exchange of files through RAP for HKSCC **Nominee and Issuer Services** used by **Share Registrars**. Under this use case, RAP supports file download and submission for the relevant services. Each Share Registrar is required to maintain its own RAP setup.

This Annex should be read together with the common requirements set out in Part II of this guide.

C2. RAP User Account Registration / Maintenance

Requests for RAP user account registration or maintenance should be submitted through **Client Connect** using the **e-Service TechS 8**.

C3. RAP User Account Model

The **maximum number of RAP user accounts** available to Share Registrars, together with the applicable **user account naming convention**, are summarised below.

User Type	Maximum Number of RAP User Accounts	Maximum Number of workstations per RAP user accounts	User Account Naming Convention
Share Registrars	2	2	Format: CRnn001, where Rnn is the Share Registrar code. The user account must be entered in capital letters .

Users are required to log on using the assigned user account exactly as provided, including case sensitivity.

Each RAP user account should be used together with its corresponding SSH private key.

C4. Public Key Naming Convention and Submission Requirements

For each RAP user account, users should generate a **dedicated SSH key pair** comprising a private key and a corresponding public key.

Each public key must be saved in a separate file and named in accordance with the RAP user account to which it relates. The **public key file, together with its fingerprint and the IP address(es) of the designated RAP client workstation(s)**, should be submitted via Client Connect for registration. Private keys must not be submitted to HKEX.

The required public key file naming convention is as follows:

CRnn001.pub — public key for RAP user account CRnn001, where Rnn represents the Share Registrars code.

Users should ensure that the public key file name matches exactly the corresponding RAP user account.

C5. Service Hours and Availability Window

Service Days	Service Hours
Monday to Friday (including weekday public holidays)	07:00 – 24:00
Saturday (including public holidays)	07:00 – 14:00

Files transferred from HKEX to Users are made available for the **past 7 calendar days** from the date of generation.

Users should also observe the service hours and schedules of the relevant interface files as documented in the corresponding File Interface Specification.

C6. Folder Structure

Each RAP user account has three default folders in RAP. The folder structure and usage principles are described below.

Folder	Description
/download	For file distribution from HKEX to Share Registrars
/submission	For file submission by Share Registrars to HKEX
/key_management	For submission of public keys for renewal

The RAP user accounts under the same Share Registrar share the same /download folder. Accordingly, the two RAP user accounts may retrieve the same set of files distributed by HKEX.

The /submission folder is assigned individually to each RAP user account and is not shared with other RAP users. The /key_management folder is also assigned individually to each RAP user account and is not shared.

The service window of each download / submission sub-folder is aligned with the RAP service hours and availability window (refer to C5). **File submissions are only allowed within the service window**; otherwise, the **submission will be rejected**, and a Reject File will be generated. **Files in download sub-subfolder are accessible only during the service window**, and the sub-folder will be **empty outside the folder service hours**.

C7. Service-Specific Download Folders

The RAP download folders available under this use case are summarised below.

Service	RAP Folder	Reference Section
EIPO (FINI)	/download/FINI	C9
Corporate Representative / Proxy / Corporate Communication	/download/HKSCC_NOMINEE	
USM ³	/download/HKSCC_USM	

C8. Service-Specific Submission Folders

The RAP submission folders available under this use case are summarised below.

Service	RAP Folder	Reference Section
EIPO (FINI)	/submission/FINI	C10
USM ²	/submission/HKSCC_USM	

³ Available to USM user

C9. Detailed File Matrix – Download

The detailed download file matrix for this use case is summarized below.

#	Download Files	Folder
1	List of files from FINI - Autopay Brokerage File (HKD) - Autopay Brokerage File (USD) - Autopay Brokerage File (CNY) - EIPO Application file - EIPO Application Report - PO Final Allocation File	/download/FINI
2	List of files from HKSCC (NOMINEE Files) - Corporate Representative or Proxy file - Corporate Communication Mailing Label file	/download/HKSCC_NOMINEE
3	List of files from HKSCC (USM Files) ⁴ - Demat Request [DM01-01] <RPID>_DEMATREQ_<yymmddhhmmss>.TXT - Demat With Transfer Request [DM01-03] <RPID>_DETRFREQ_<yymmddhhmmss>.TXT - Certificate Range Details [DM01-05] <RPID>_CRTRGDTL_<yymmddhhmmss>.TXT - Transfer Request (HKSCCN) [UT01-01] <RPID>_TRFREQHK_<yymmddhhmmss>.TXT	/download/HKSCC_USM

⁴ Available to USM user

- Share Movement Request After Repurchase of Shares [SM01-01] <RPID>_SMREPREQ_<yymmddhhmmss>.TXT - Day-end Control File [CN01-01] <RPID>_CNTLFILE_<yymmddhhmmss>.TXT - Event Reference Number [CA01-08] <RPID>_EVENTREF_<yymmddhhmmss>.TXT - Proxy Instruction [CA01-09] <RPID>_PXYINSTR_<yymmddhhmmss>.TXT - Corporate Representative [CA01-10] <RPID>_CORPREPR_<yymmddhhmmss>.TXT - Subscription [CA01-11] <RPID>_SUBINSTR_<yymmddhhmmss>.TXT - Exercise Instruction [CA01-12] <RPID>_EXCINSTR_<yymmddhhmmss>.TXT - Takeover Instruction [CA01-13] <RPID>_TKOINSTR_<yymmddhhmmss>.TXT - Election Instruction [CA01-14] <RPID>_ELTINSTR_<yymmddhhmmss>.TXT	
---	--

C10. Detailed File Matrix – Submission

The detailed submission file matrix for this use case is summarized below.

Submission of PO Allotment File

RAP Folder	/submission/FINI
Filename Convention	PO_ALLOT_<SSSSSSSSSS>

	where <SSSSSSSSSS> is the stock code in 10 characters with left trailing spaces
File Extension Allowed	ZIP
Auto-append String in Acknowledgement File Filename	_ <identity_code> 001

Submission of EIPO Bonus Allotment File

RAP Folder	/submission/FINI
Filename Convention	PO_BONUS_<SSSSSSSSSS> where <SSSSSSSSSS> is the stock code in 10 characters with left trailing spaces
File Extension Allowed	ZIP
Auto-append String in Acknowledgement File Filename	_ <identity_code> 001

Submission of USM File⁵

RAP Folder	/submission/HKSCC_USM
Filename Convention	- Demat Request Completion Confirmation [DM01-02] <RPID>_DEMATCFM_<yymmddhhmmss>.TXT - Demat With Transfer Completion Confirmation [DM01-04] <RPID>_DETRFCFM_<yymmddhhmmss>.TXT - Certificate Range Rejection Details [DM01-06] <RPID>_CRTRGREJ_<yymmddhhmmss>.TXT - Confirmation of Transfer Completion (HKSCCN) [UT01-02]

⁵ Available to USM user

<RPID>_TRFCFMHK_<yymmddhhmmss>.TXT

- Confirmation of Share Movement After Repurchase of Shares [SM01-02]

<RPID>_SMREPCFM_<yymmddhhmmss>.TXT

- Daily Shareholding Confirmation for HKSCCN Holdings [SC01-01]

<RPID>_HKSCCN SH_<yymmddhhmmss>.TXT

- ROM Update Confirmation [CA01-01]

<RPID>_ROMUPCFM_<yymmddhhmmss>.TXT

- Cash Payment Notification [CA01-02]

<RPID>_CASHPCFM_<EVENTREF>
_<yymmddhhmmss>.TXT

- Entitlement [CA01-03]

<RPID>_CAPDENTL_<EVENTREF>_<yymmddhhmmss>
.TXT

- PAL / EAF [CA01-04]

<RPID>_PALEAFET_<EVENTREF>_<yymmddhhmmss>
.TXT

- ROM Update for Sub-division and Consolidation (Conditional) [CA01-05]

<RPID>_RUSUBCSD_<yymmddhhmmss>.TXT

- Entitled Holdings [CA01-06]

<RPID>_ELDHOLDG_<EVENTREF>_<yymmddhhmmss>
.TXT

- ROM Update for Placing [CA01-07]

<RPID>_RUPLCCFM_<SSSSSSSSSS>_<yymmddhhmmss>
.TXT

- Confirmation and Rejection [CA01-15]

	<RPID>_CACFMREJ_<yymmddhhmmss>.TXT - Takeover Confirmation [CA01-16] <RPID>_TKOIRESP_<yymmddhhmmss>.TXT - Instruction Response [CA01-17] <RPID>_CAINSRSP_<yymmddhhmmss>.TXT <RPID> stands for Registrar Participant ID <yymmddhhmmss> stands for the timestamp of the files being generated, yy is the year, 1st mm is the month, dd is the date, hh is the hour, 2nd mm is the minutes and ss is the second, e.g., the file with timestamp 180806144205 means the file is generated on 6th August 2018 at 14:42:05. <EVENTREF> stands for the Event Reference Number with format 'A'+ 8 digits. _<SSSSSSSSSS> stands for the 10-characters stock code for Post Listing – Placing. e.g. for stock code 700, it will be '700 '.
File Extension Allowed	TXT
Auto-append String in Acknowledgement File Filename	_<identity_code>001

C11. File Submission

Users submit files to HKEX by **uploading the relevant files to the applicable /submission/<sub-folder> in RAP**. After submission, files are collected and removed from the submission folder immediately, or according to the schedule specified in the corresponding File Interface Specification. Upon completion of processing, the system generates either an Acknowledgement File (.rcvd) or a Rejection File (.rej).

Each submitted file is subject to the following validation checks:

- the **file name, file extension and submission time** must comply with the rules defined

for the relevant submission folder;

- the **identity code embedded in the file name** must be one of the identity codes entitled to the submitting RAP user account; and
- the **file size must not exceed the file size limit of 500MB**.

Users should note the following operational considerations:

- **file renaming functions using RAP rename commands are not supported**; users should ensure that any SFTP client feature that uploads a temporary file name and subsequently renames the file (for example, certain WinSCP settings) is disabled;
- acknowledgement and rejection files are generated on a per RAP user account basis;
- acknowledgement and rejection files are retained for a maximum of **24 hours** and are subsequently **removed by the end-of-day housekeeping job**; and
- if the file name is longer than the system limit of 128 characters, the file will be rejected at SFTP level and no `.rej` file will be generated.

The **Acknowledgement File** (`.rcvd`) generated to the `/submission/<sub-folder>` is a **positive acknowledgement** indicating that the submitted file has been accepted.

The file name is formatted as:

```
<original file name><auto-appended string>.<suffix>.<timestamp-
HHMMSS>.<seq>.rcvd
```

where the optional sequence number `.<seq>` is appended only when multiple files with the same file name are uploaded within same second and are accepted. The `<auto-appended string>` is determined by the folder-specific setting.

For example, if 3 files with the same file name are uploaded within same second and accepted, the `.rcvd` file will be named as:

1st file: `<original file name><auto-appended string>.<suffix>.<timestamp-HHMMSS>.rcvd`

2nd file: `<original file name><auto appended string>.<suffix>.<timestamp-HHMMSS>.1.rcvd`

3rd file: `<original file name><auto appended string>.<suffix>.<timestamp-HHMMSS>.2.rcvd`

The `.rcvd` file is a fixed-width text file in Windows text file format (CR+LF line ending) and

contains the following fields:

#	Field	Type	Size	Remarks
1	Checksum	Alphanumeric	66	SHA-256 checksum of the submitted file for verification
2	Filename	Alphanumeric	128	Filename of the submitted file

The **Rejection File** (.rej) generated to the /submission/<sub-folder> is a **negative acknowledgement** indicating that the submitted file has been rejected.

The filename is formatted as:

<original file name>.<timestamp-HHMMSS>[.seq].rej

For example, if 3 files with the same file name are uploaded within same second and rejected, the .rej file will be named as:

1st file: <original file name>.<timestamp-HHMMSS>.rej

2nd file: <original file name>.<timestamp-HHMMSS>.1.rej

3rd file: <original file name>.<timestamp-HHMMSS>.2.rej

The .rej file is a text file in Windows text file format (CR+LF line ending) and contains the following fields:

#	Field	Type	Size	Remarks
1	Reject Code	Numeric	5	Reject code
2	Reject Message	Alphanumeric	255	Reject Message in English

C12. Connectivity Details

RAP is accessible only through the **Securities and Derivatives Network (SDNet/2)** designated for connection to RAP.

RAP client workstations must be configured with IP addresses that fall within the same SDNet/2 subnet for HKSCC. The applicable subnet ranges are summarised below.

SDNet IP Addresses Subnet	Remarks
10.135.0.0/16 10.136.0.0/16	Applicable to R03, R39, R41, R45 only
10.71.0.0/17 10.71.128.0/17	Applicable to all (except the above)

Users may connect to RAP directly using the applicable IP addresses of the HKSCC RAP.

Primary Data Centre	Secondary / Backup Data Centre	Remarks
10.243.2.141 port 18801	10.243.66.141 port 18801	Applicable to R03, R39, R41, R45 only
10.243.2.142 port 18801	10.243.66.142 port 18801	
10.241.42.101 port 18801	10.241.142.101 port 18801	Applicable to all (except the above)
10.241.42.102 port 18801	10.241.142.102 port 18801	

In a contingency situation, users will be notified to connect to the secondary / backup data centre. Users should check the `/submission/` sub-folder to confirm that their submitted files have been successfully received. There is a possibility that files submitted during an SFTP service failure may be lost during the data center switch. In such cases, users are required to resubmit the files.

C13. Enquiries and Support

For any enquiries from Share Registrars under this use case, Share Registrars please contact their usual business contact point within HKEX Operations Division.

Annex D – HKCC / SEOCH DCASS and CCMS Reports-Specific Guidelines

D1. Purpose and Applicability

This Annex sets out the use case-specific technical and operational requirements applicable to the retrieval of **DCASS reports**, **pre-trade risk management reports** and **CCMS reports** through RAP by **HKCC and SEOCH Clearing Participants**.

This Annex should be read together with the common requirements set out in Part II of this guide.

D2. RAP User Account Registration / Maintenance

Requests for RAP user account registration or maintenance should be submitted through **Client Connect** using the **e-Service TechS 8**.

D3. RAP User Account Model

The **maximum number of RAP user accounts** available to Clearing Participants, together with the applicable **user account naming convention**, are summarised below.

User Type	Maximum Number of RAP User Accounts	Maximum Number of workstations per RAP user accounts	User Account Naming Convention
Clearing Participants	4	4	Format: DCXXX001, where CXXX is the DCASS customer code of the Clearing Participant. The user account must be entered in capital letters .

Users are required to log on using the assigned user account exactly as provided, including case sensitivity.

Each RAP user account should be used together with its corresponding SSH private key.

D4. Public Key Naming Convention and Submission Requirements

For each RAP user account, users should generate a **dedicated SSH key pair** comprising a private key and a corresponding public key.

Each public key must be saved in a separate file and named in accordance with the RAP user account to which it relates. The **public key file, together with its fingerprint and the IP address(es) of the designated RAP client workstation(s)**, should be submitted via Client Connect for registration. Private keys must not be submitted to HKEX.

The required public key file naming convention is as follows:

DCXXX001.pub — public key for RAP user account DCXXX001, where CXXX represents the DCASS customer code.

Users should ensure that the public key file name matches exactly the corresponding RAP user account.

D5. Service Hours and Availability Window

Report Type	Service Days	Service Hours
DCASS and pre-trade risk management reports	Trading days	07:00 – 03:30
CCMS Reports	Trading days	07:15 – 24:00
	Saturday (except public holidays)	07:15 – 13:00

Reports and files are made available for the **past 10 calendar days** from the date of generation. Users should retrieve and save the required reports and files in a timely manner for daily operational use.

D6. Folder Structure

Each RAP user account may access up to 5 RAP folders, depending on the type of reports assigned to that user account. The folder structure and usage principles are described below.

Folder	Description
/download/DCASS	For retrieval of DCASS daily and monthly reports / files applicable to the Clearing Participant.
/download/DCASS_OTHERS	For retrieval of other reports / files applicable to the Clearing Participant for the derivatives market.
/download/HKCC_SEOCH_CCMS_GLOB	For retrieval of common CCMS reports / files applicable to all Clearing Participants and CCMS reports / files applicable to the specific Clearing Participant for both HKCC and SEOCH.

/key_management/publickey	Used for submission of public key for key renewal. Each RAP user account is assigned a dedicated key_management folder, which must not be shared with other RAP user accounts.
/submission	<i>Not applicable.</i>

Notes:

- If the RAP user account of a Clearing Participant is configured to receive DCASS reports, the account can access both /download/DCASS and /download/DCASS_OTHERS.
- If the RAP user account of a Clearing Participant is configured to receive CCMS reports, the account can access /download/HKCC_SEOCH_CCMS_GLOB.

D7. Connectivity Details

RAP is accessible only through the **Securities and Derivatives Network (SDNet/2) or HKEX Service Network (HSN)**.

RAP client workstations must be configured with IP addresses that fall within the same SDNet/2 subnet for DCASS or HSN. The applicable subnet ranges are summarised below.

SDNet IP Addresses Subnet	
10.132.0.0/16	172.18.0.0/16
10.133.0.0/16	172.19.0.0/16
10.217.0.0/16	172.20.0.0/16
	172.21.0.0/16

Users may connect to RAP directly using the applicable IP addresses of the HKCC/ SEOCH RAP.

Primary Data Centre	Secondary / Backup Data Centre
10.151.14.141 port 18801	10.152.14.141 port 18801
10.151.14.142 port 18801	10.152.14.142 port 18801

D9. Enquiries and Support

For any enquiries regarding the use of RAP for retrieving HKCC / SEOCH DCASS and CCMS reports, please contact us through the channels below:

Email: clearingpsd@hkex.com.hk / Hotline: 2979 7222

Annex E – OTC Clear OASIS Reports and Direct Messaging-Specific Guidelines

E1. Purpose and Applicability

This Annex sets out the use case-specific technical and operational requirements applicable to the retrieval of **OTC Clear OASIS reports** through SFTP and, where applicable, the use of **Direct Messaging Service** through SFTP for OTC Clear workflows.

Under this use case, the RAP is provided by OTC Clear to **Clearing Members, Clearing Brokers and Sponsored Settlement Members** for report retrieval. In addition, the Direct Messaging Service supports the functions of notification of trade clearing results and clearing take-up process of client trades.

This Annex should be read together with the common requirements set out in Part II of this guide.

E2. RAP User Account Registration / Maintenance

Requests for RAP user account registration or maintenance should be submitted to OTC Clear Operations Team using the form [“Request for the use of SFTP report download service or SFTP/ MQ direct messaging service”](#).

E3. RAP User Account Model

The **maximum number of RAP user accounts** available to Clearing Members, Clearing Brokers and Sponsored Settlement Members, together with the **maximum number of workstations per accounts**, are summarised below.

User Type	Maximum Number of RAP User Accounts	Maximum Number of workstations per RAP user accounts	User Account Naming Convention
Clearing Members/ Clearing Brokers/ Sponsored Settlement Members	3	4	Format: OABCDEFGH123T001, where ABCDEFGH123T is the OCASS id. The user account must be entered in capital letters.

Users are required to log on using the assigned user account exactly as provided, including case sensitivity.

Each RAP user account should be used together with its corresponding SSH private key.

E4. Public Key and Submission Requirements

For each RAP user account, users should generate a **dedicated SSH key pair** comprising a private key and a corresponding public key.

Each public key must be saved in a separate file. The **public key file and the IP address(es) of the designated RAP client workstation(s)**, should be submitted to OTC Clear Operations Team by email: OTC_Operations@hkex.com.hk. Private keys must not be submitted to HKEX.

The required public key file naming requirements follow section 5.3.

E5. Service Hours and Availability Window

The OTC Clear RAP service hours are Sunday 07:00 to the following Saturday 07:00 (HKT).

Reports and files are made available for the **past 18 calendar days** from the date of generation. Users should retrieve and save the required reports and files in a timely manner for daily operational use.

E6. Folder Structure

For OASIS reports, the following download folders are used. Please refer to the Technical Specification for Direct Messaging Service for the relevant message download and submission folders.

Reports Folders

Folder	Description
/download/OTC_HOUSE/yyyymmdd	For House Activity Reports.
/download/OTC_CLIENT/yyyymmdd	For Client Clearing Activity Reports.
/download/OTC_SSM/yyyymmdd	For Sponsored Settlement Member (SSM) Client Activity Reports.

Common Folders

Folder	Description
/key_management/publickey	Used for submission of public keys for key renewal. Each RAP user account is assigned a dedicated <code>key_management</code> folder, which must not be shared with other RAP user accounts.

/submission	<i>Not applicable.</i>
-------------	------------------------

Notes:

- `yyyymmdd` represents the system-generated subfolder for each calendar day. Reports and files generated on a specific day are made available under the corresponding date subfolder.
- OASIS reports are delivered to the RAP account at specific time intervals each day, roughly hourly. The exact time of report publication in the RAP may fluctuate from day to day based on business volume and system run time.
- Users are not allowed to update or remove any files from the download folder.

E7. Reports and File Name Format

For the House and Client report folders, three ZIP files are generally provided each day: SOD, INT and EOD. Their indicative time groupings are as follows:

ZIP File Type	File Name Pattern	Indicative Report Generation Time Included	Mode
SOD	SOD_yymmdd_<Account Name>.zip	04:00 to 08:45 (HKT)	Append
Intraday	INT_yymmdd_<Account Name>.zip	08:45 to 20:00 (HKT)	Append
EOD	EOD_yymmdd_<Account Name>.zip	20:00 to 04:00 (HKT)	Append

The file name format for the reports in the ZIP files are as below:

House Activity Report

- reportname_99999999_yyyy-mm-dd hh-mm-ss AM.csv **or**
- reportname_99999999_yyyy-mm-dd hh-mm-ss PM.csv

Client Activity Report

- reportname_C_99999999_yyyy-mm-dd hh-mm-ss AM.csv **or**
- reportname_C_99999999_yyyy-mm-dd hh-mm-ss PM.csv

Notes:

- 99999999 is the sequence number generated by OCASS.
- The **EOD ZIP file** is normally ready for download **after 22:00**.
- In the Member Testing environment, reports will be provided on request basis, and the file structure may be different.

Clearing members would also be able to access the Sponsored Settlement Member (SSM) Client Activity Reports. Three ZIP files are summarized as follows:

ZIP File Type	File Name Pattern	Indicative Report Generation Time Included	Mode
SOD	SOD_yymmdd_<SSM_Account Name>.zip	04:00 to 08:45 (HKT)	Append
Intraday	INT_yymmdd_<SSM_Account Name>.zip	08:45 to 20:00 (HKT)	Append
EOD	EOD_yymmdd_<SSM_Account Name>.zip	20:00 to 04:00 (HKT)	Append

Notes:

- The **EOD ZIP** file is normally ready for download **after 22:00**.

E8. Connectivity Details

OTC Clear RAP are accessible through **Securities and Derivatives Network (SDNet/2)**. Where a user workstation is already connected to OASIS via SDNet/2, the same workstation may be used to access the RAP, subject to the appropriate firewall configuration and IP address registration.

Members must ensure that:

- SFTP connections originate from pre-registered source IP addresses assigned to the Member;
- where Network Address Translation (NAT) is used, the source IP address is translated into the registered SDNet/2 range; and
- firewall rules allow outbound and inbound traffic to the designated OTC Clear RAP IP addresses using the required port.

The applicable subnet ranges are summarized below.

SDNet IP Addresses Subnet
PCCW - 10.58.0.0/24 to 10.58.127.0/24
HKBNES - 10.59.0.0/24 to 10.59.127.0/24

Users may connect to Production RAP directly using the applicable IP addresses of the OTC Clear RAP. **If users cannot connect to RAP, they should download the reports using OASIS.** Also, they should inform OTC Clear if further help is needed.

Primary Data Centre	Secondary / Backup Data Centre
10.154.11.141 port 18801	10.153.11.141 port 18801
10.154.11.142 port 18801	10.153.11.142 port 18801

For RAP's development environment, the applicable IP address is 10.154.11.141 port 18801.

E9. Recommendations

This section sets out recommended steps for connecting to OTC Clear RAP.

Step 1: Connect to SDNet/2 Routers

Step 1.1:

Before the configuration, please ensure that the Metro Ethernet communication lines and routers have been installed and configured properly by the SDNet/2 service provider already.

Step 1.2:

Connect the SDNet/2 routers to the LAN switches with LAN cables. The LAN interface of the SDNet/2 router supports network speed up to Gigabit Ethernet and it is configured as “Auto Negotiation” (i.e. both speed and duplex mode are auto). The LAN switch ports (connecting the SDNet/2 routers) should also have “auto” configuration settings and should provide a single VLAN (Layer 2) for connecting SDNet/2 router and the SFTP client.

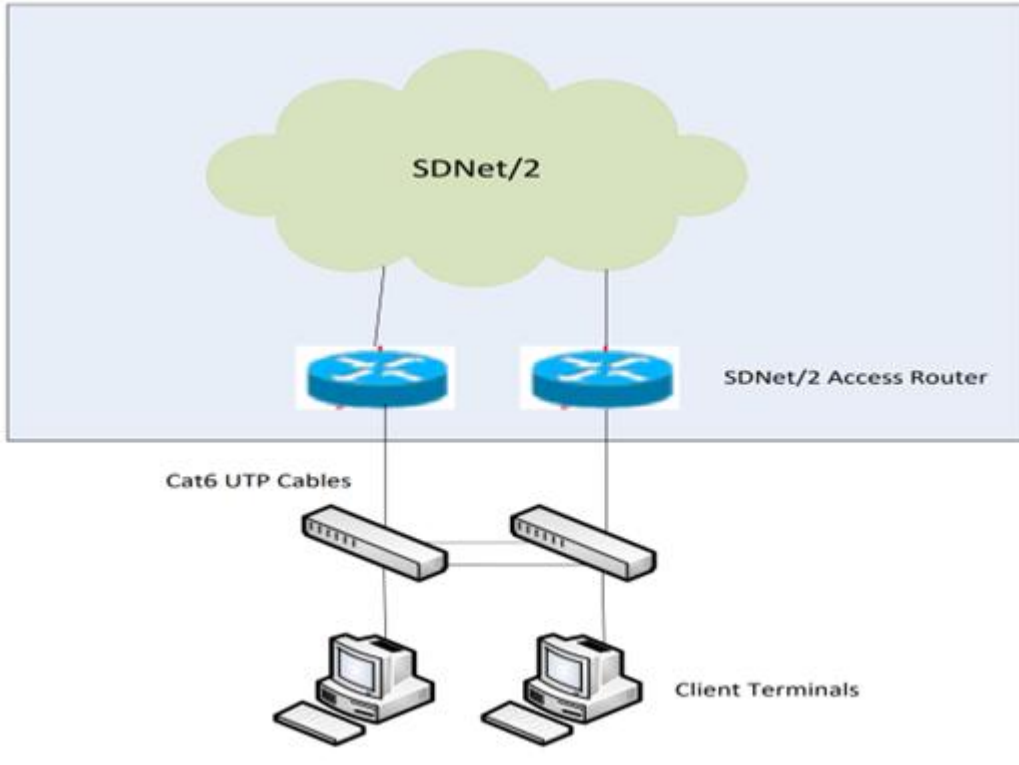
Step 1.3:

HSRP/VRRP group number on SDNet/2 router for OASIS will be assigned by the SDNet/2 service vendor. Users should avoid using the same HSRP/VRRP group number in their network for applications other than OASIS.

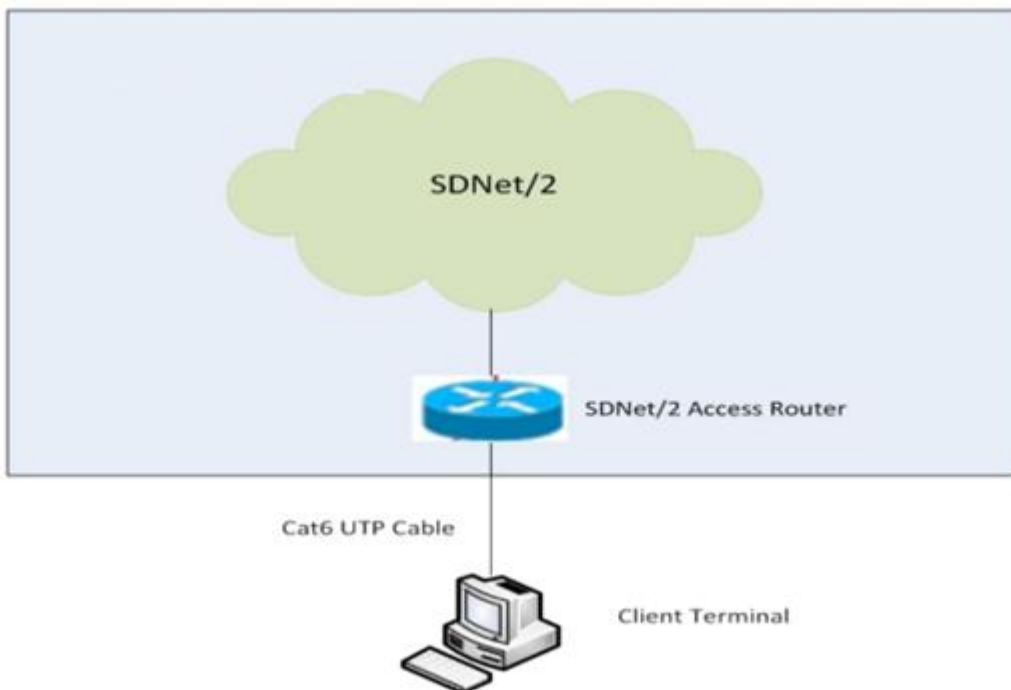
Step 1.4:

Connect the PC/Server to the routers and LAN switch with LAN cables. There are two possible options to establish the connection:

Option 1: Dual-link connection (for production site)



Option 2: Single-link connection



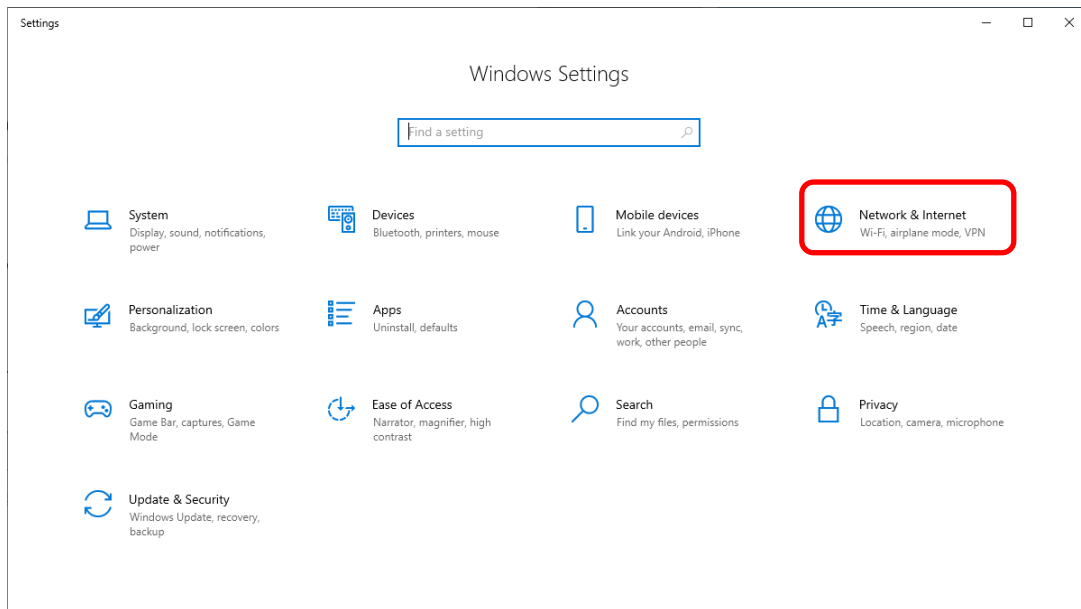
Step 2: Firewall Setup

The following IP addresses and ports need to be opened on the firewall for access to the production RAP in section E8.

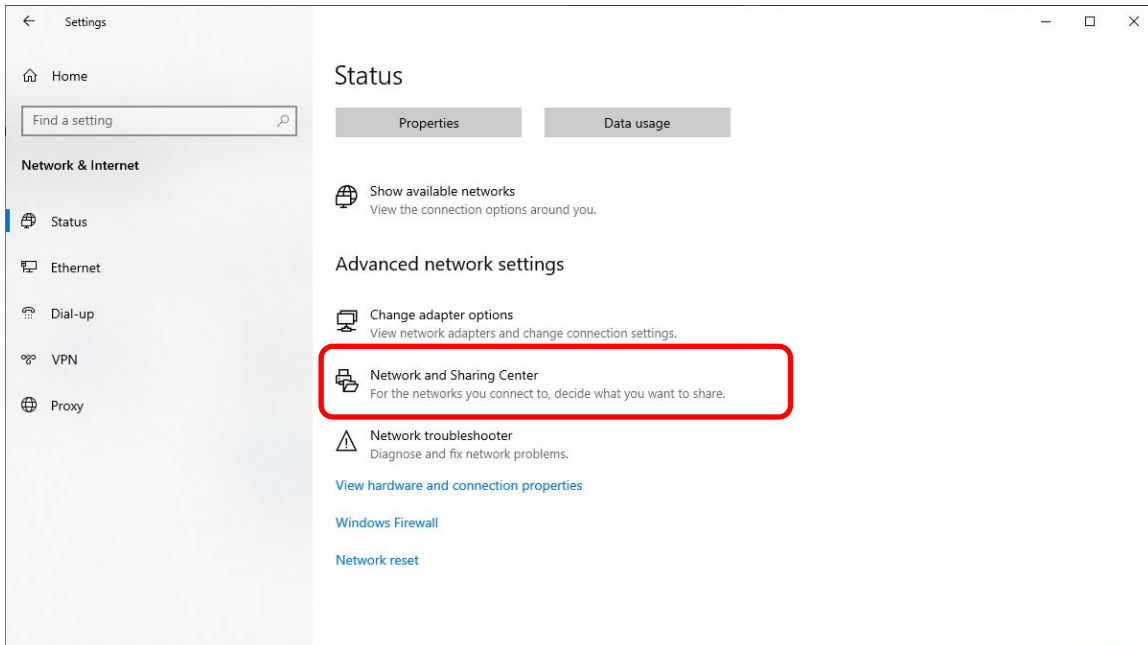
TCP/IP and Ethernet Card Configuration (for Windows 10 PC)

Step 1: Login in as an administrator to perform the following procedures.

Step 2: Click **“Start”**, go to the **“Control Panel”**, and then select **“Network & Internet”**:

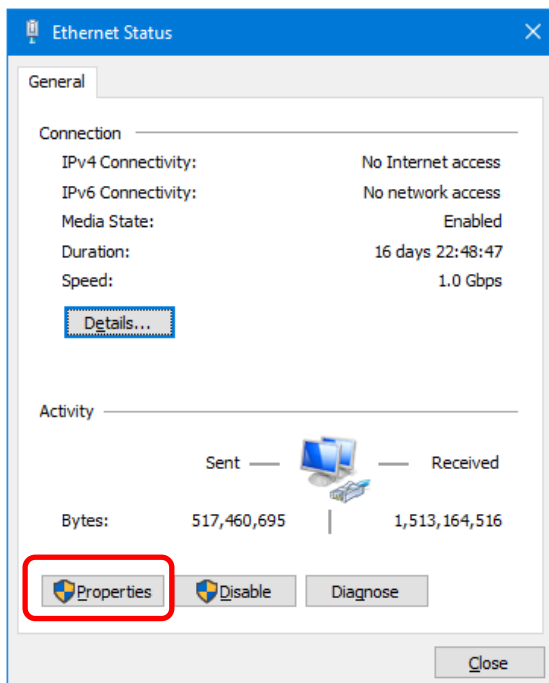


Step 3: Under **“Advanced”**, click the **“Network and Sharing Center”**:

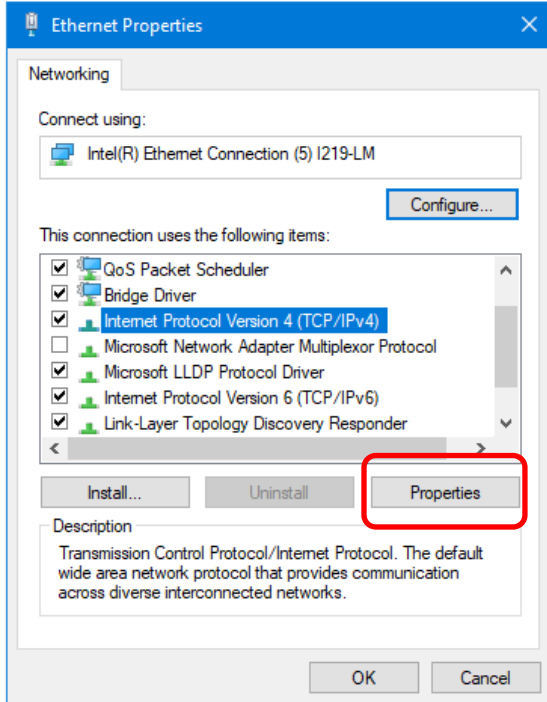


Step 4: Under “View your active networks”, click the Connections you would like to configure. Depending on your current settings, it may be called “Ethernet” or “Local Area Network”.

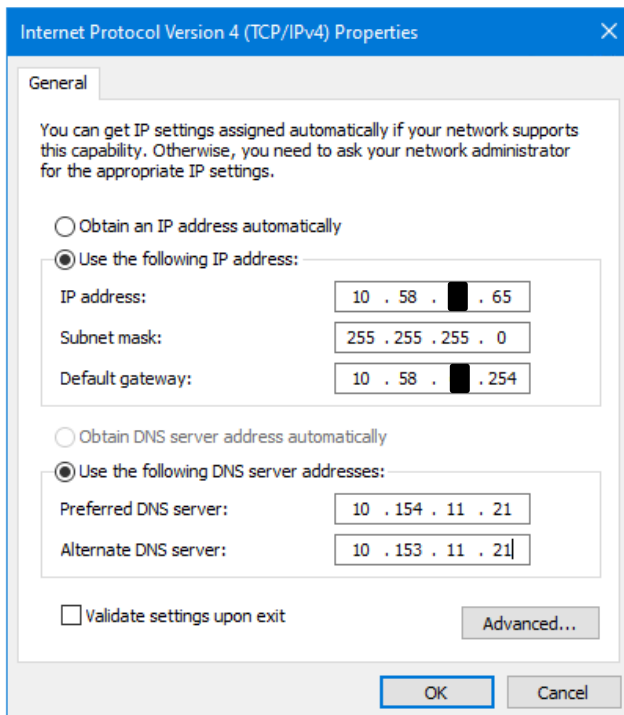
Step 5: In the Status window (e.g. “Ethernet Status”), click the “Properties” button.



Step 6: Select “Internet Protocol Version 4 (TCP/IP)” and click the “Properties”.



Step 7: Select “Use the following IP address” radio button and enter the following information:



1. Enter the “IP address” and “Default gateway” assigned by your SDNet/2 service provider.

2. Enter "255.255.255.0" for "Subnet mask".
3. If you would also use OASIS on this PC, you may select the "Use the following DNS server addresses" radio button and enter the "Preferred DNS server" and "Alternate DNS server" as set out in the Step 2.2 of the OASIS Configuration Guide.
4. Click "OK".

Step 8: Add static routes

1. Open a command prompt
2. Issue the following commands (please use the "Default gateway" assigned by your SDNet/2 service provider instead of x.x.x.254):

<pre>route add -p 10.153.11.0 mask 255.255.255.0 x.x.x.254 route add -p 10.154.11.0 mask 255.255.255.0 x.x.x.254</pre>
--

Step 9: Restart the Windows PC

Reference information

The following range of IP address / subnet mask may be assigned by SDNet/2 service providers (in CIDR):

- PCCW - 10.58.0.0/24 to 10.58.127.0/24
- HKBNES - 10.59.0.0/24 to 10.59.127.0/24

The last number in the IP address may be x.x.x.65 ~ x.x.x.190.

E10. Enquiries and Support

For any enquiries regarding the use of RAP for retrieving OASIS reports and Direct Messaging Service, please contact us through the channels below:

Email: OTC_Operations@HKEX.COM.HK / Hotline: 2211 6508

Annex F – HKSCC USM Services (for IRD)-Specific Guidelines

F1. Purpose and Applicability

This Annex sets out the use cases, specific technical and operational requirements applicable to the exchange of files through RAP in support of USM by **IRD**. Under this use case, RAP supports file download and submission for stamp duty processing under USM services. User is required to maintain its own RAP setup.

This Annex should be read together with the common requirements set out in Part II of this guide.

F2. RAP User Account Registration / Maintenance

Requests for RAP user account registration or maintenance should be submitted via email to cs_cps_cc@hkex.com.hk with G-Form 21 attached.

F3. RAP User Account Model

The **maximum number of RAP user accounts** available to IRD, together with the applicable **user account naming convention**, are summarised below.

User Type	Maximum Number of RAP User Accounts	Maximum Number of workstations per RAP user accounts	User Account Naming Convention
IRD	2	2	Format: CIRD001 and CIRD002. The user account must be entered in capital letters .

Users are required to log on using the assigned user account exactly as provided, including case sensitivity.

Each RAP user account should be used together with its corresponding SSH private key.

F4. Public Key Naming Convention and Submission Requirements

For each RAP user account, users should generate a **dedicated SSH key pair** comprising a private key and a corresponding public key.

Each public key must be saved in a separate file and named in accordance with the RAP user account to which it relates. The **public key file, together with its fingerprint and the IP address(es) of the designated RAP client workstation(s)**, should be submitted via email to cs_cps_cc@hkex.com.hk for registration. Private keys must not be submitted to HKEX.

The required public key file naming convention is as follows:

CIRD001.pub — public key for RAP user account CIRD001.

Users should ensure that the public key file name matches exactly the corresponding RAP user account.

F5. Service Hours and Availability Window

Service Days	Service Hours
Monday to Friday (including weekday public holidays)	07:00 – 24:00
Saturday (including public holidays)	07:00 – 14:00

Files transferred from HKEX to users are made available for the **past 7 calendar days** from the date of generation.

Users should also observe the service hours and schedules of the relevant interface files as documented in the corresponding File Interface Specification.

F6. Folder Structure

Each RAP user account has three default folders in RAP. The folder structure and usage principles are described below.

Folder	Description
/download/HKSCC_USM	For USM file distribution from HKEX to IRD
/submission/HKSCC_USM	For USM file submission by IRD to HKEX
/key_management	For submission of public keys for renewal

The RAP user accounts share the same /download folder. Accordingly, the two RAP user accounts may retrieve the same set of files distributed by HKEX.

The /submission folder is assigned individually to each RAP user account and is not shared with other RAP users. The /key_management folder is also assigned individually to each RAP user account and is not shared.

Users may refer to “Stamp Duty Interface Spec – HKEX and IRD” for the detailed list of files and the relevant requirements.

The service window of each download / submission sub-folder is aligned with the RAP service hours and availability window (refer to F5). **File submissions are only allowed within the service window**; otherwise, the **submission will be rejected**, and a Reject File will be generated. **Files in download sub-subfolder are accessible only during the service window**, and the sub-folder will be **empty outside the folder service hours**.

F7. File Submission

Users submit files to HKEX by **uploading the relevant files to the applicable /submission/<sub-folder> in RAP**. After submission, files are collected and removed from the submission folder immediately, or according to the schedule specified in the corresponding File Interface Specification. Upon completion of processing, the system generates either an Acknowledgement File (`.rcvd`) or a Rejection File (`.rej`).

Each submitted file is subject to the following validation checks:

- the **file name, file extension and submission time** must comply with the rules defined for the relevant submission folder;
- the **identity code embedded in the file name** must be one of the identity codes entitled to the submitting RAP user account; and
- the **file size must not exceed the file size limit of 500MB**.

Users should note the following operational considerations:

- **file renaming functions using RAP rename commands are not supported**; users should ensure that any SFTP client feature that uploads a temporary file name and subsequently renames the file (for example, certain WinSCP settings) is disabled;
- acknowledgement and rejection files are generated on a per RAP user account basis;
- acknowledgement and rejection files are retained for a maximum of **24 hours** and are subsequently **removed by the end-of-day housekeeping job**; and
- if the file name is longer than the system limit of 128 characters, the file will be rejected at SFTP level and no `.rej` file will be generated.

The **Acknowledgement File** (`.rcvd`) generated to the `/submission/<sub-folder>` is a **positive acknowledgement** indicating that the submitted file has been accepted.

The file name is formatted as:

```
<original file name><auto-appended string>.<suffix>.<timestamp-
HHMMSS>.<seq>.rcvd
```

where the optional sequence number `.<seq>` is appended only when multiple files with the same file name are uploaded within same second and are accepted. The `<auto-appended string>` is determined by the folder-specific setting.

For example, if 3 files with the same file name are uploaded within same second and accepted, the `.rcvd` file will be named as:

1st file: <original file name><auto-appended string>.<suffix>.<timestamp-HHMMSS>.rcvd

2nd file: <original file name><auto appended string>.<suffix>.<timestamp-HHMMSS>.1.rcvd

3rd file: <original file name><auto appended string>.<suffix>.<timestamp-HHMMSS>.2.rcvd

The .rcvd file is a fixed-width text file in Windows text file format (CR+LF line ending) and contains the following fields:

#	Field	Type	Size	Remarks
1	Checksum	Alphanumeric	66	SHA-256 checksum of the submitted file for verification
2	Filename	Alphanumeric	128	Filename of the submitted file

The **Rejection File** (.rej) generated to the /submission/<sub-folder> is a **negative acknowledgement** indicating that the submitted file has been rejected.

The filename is formatted as:

<original file name>.<timestamp-HHMMSS>[.seq].rej

For example, if 3 files with the same file name are uploaded within same second and rejected, the .rej file will be named as:

1st file: <original file name>.<timestamp-HHMMSS>.rej

2nd file: <original file name>.<timestamp-HHMMSS>.1.rej

3rd file: <original file name>.<timestamp-HHMMSS>.2.rej

The .rej file is a text file in Windows text file format (CR+LF line ending) and contains the following fields:

#	Field	Type	Size	Remarks
1	Reject Code	Numeric	5	Reject code
2	Reject Message	Alphanumeric	255	Reject Message in English

F8. Connectivity Details

RAP is accessible only through the **Securities and Derivatives Network (SDNet/2)** designated for connection to RAP.

RAP client workstations must be configured with IP addresses that fall within the same SDNet/2 subnet for HKSCC. The applicable subnet ranges are summarised below.

SDNet IP Addresses Subnet
10.71.0.0/17 10.71.128.0/17

Users may connect to RAP directly using the applicable IP addresses of the HKSCC RAP.

Primary Data Centre	Secondary / Backup Data Centre
10.241.42.101 port 18801	10.241.142.101 port 18801
10.241.42.102 port 18801	10.241.142.102 port 18801

In a contingency situation, Users will be notified to connect to the secondary / backup data centre. Users should check the `/submission/` sub-folder to confirm that their submitted files have been successfully received. There is a possibility that files submitted during an SFTP service failure may be lost during the data center switch. In such cases, users are required to resubmit the files.

F9. Enquiries and Support

For any enquiries from IRD under this use case, Share Registrars please contact their usual business contact point within HKEX Operations Division.

Appendices

Appendix 1 – Quick Reference Matrix by Clearing House

Clearing House/ Service	Applicable Annex	Primary Purpose	RAP Functions Supported	Primary User Type
HKSCC CCASS & VaR Reports	Annex A	Retrieval of CCASS reports, VaR reports and subscribed RPF	Download	CCASS Participants, Designated Banks
HKSCC Corporate Action Instructions (for CCASS Participants)	Annex B	Submission of corporate action instruction files	Submission	CCASS Participants
HKSCC Depository, Nominee & Issuer Services (for Share Registrars)	Annex C	Exchange of Nominee, FINI, Corporate Communication and USM files	Download and Submission	Share Registrars
HKCC/ SEOCH DCASS & CCMS Reports	Annex D	Retrieval of derivatives clearing and risk-related reports	Download	HKCC/ SEOCH Clearing Participants
OTC Clear OASIS Reports & Direct Messaging	Annex E	Retrieval of OASIS reports and SFTP-based Direct Messaging	Download and Submission	OTC Clear Clearing Members, Sponsored Settlement Members, Clearing Brokers
HKSCC USM Services (for IRD)	Annex F	Exchange of stamp duty files for USM	Download and Submission	IRD

Appendix 2 – Rejection Codes used in Submission Rejection File

#	Rejection Code	Synopsis
1.	3301	Exceed daily file size limit
2.	3302	Exceed daily file upload number limit
3.	4003	Rejected by virus scan
4.	4004	Exceed file size limit
5.	4007	File name contains invalid characters
6.	4505	Invalid file name
7.	4506	Invalid file name extension
8.	4507	Beyond submission hour
9.	4508	Submission for input date is closed

Appendix 3 – SSH Protocol Algorithms

Key Exchange Algorithms	<u>curve25519-sha256@libssh.org</u> , <u>ecdh-sha2-nistp521</u> , ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
MAC Algorithms	hmac-sha2-512, hmac-sha2-512-96, hmac-sha2-256
Ciphers Algorithms	<u>aes256-gcm@openssh.com</u> , <u>aes128-gcm@openssh.com</u> , <u>aes256-ctr</u> , <u>aes128-ctr</u>
Public/Host Key Algorithms	ssh-rsa ⁶ , rsa-sha2-256, rsa-sha2-512

⁶ Public/ host key algorithm “ssh-rsa” is not applicable for the use case in HKSCC Corporate Action Instructions Services.