



**HONG KONG INTERBANK  
CLEARING LIMITED**  
香港銀行同業結算有限公司

## **Hong Kong Trade Repository**

### **Administration and Interface Development Guide**

**(Reporting Service – For the use of UTI, UPI, and the reporting of CDE in  
ISO 20022 standard (ISO 20022))**

**Publication Date: September 2024**

**Version: 1.0**

This document, which contains confidential material, is the property of The Hong Kong Monetary Authority (HKMA). It is not to be used for any other purposes, copied, distributed or transmitted in any forms or any means without the prior written consent of the HKMA.

## **DOCUMENT HISTORY**

<b>Revision Date</b>	<b>Updated By</b>	<b>Version</b>	<b>Amendment Summary</b>
September 2024	HKICL	1.0	Initial publication.

## Document References

	Document Name
[1]	SWIFT User Handbook
[1.1]	SWIFTNet Service Description (part of [1])
[1.2]	SWIFTNet Naming and Addressing Guide (part of [1])
[2]	SWIFT WebAccess Configuration and Troubleshooting Guide
[3]	Operating Procedures for HKTR - User Manual for Participants

## Abbreviations and Acronyms

Abbreviation/Acronym	Description
CDE	Critical Data Elements
CSV	Comma Separated Value
eCMT	Central MoneyMarkets Unit Member Terminal
eMBT	Member Bank Terminal
FpML	Financial products Markup Language
FTS	File Transfer Server on ICLNet
GUI	Graphical User Interface
HKICL	Hong Kong Interbank Clearing Limited
HKMA	Hong Kong Monetary Authority
HKTR	Hong Kong Trade Repository
PDF	Portable Document Format
PDU	Protocol Data Units
SWIFT	Society Worldwide Interbank Financial Telecommunication
AWP	SWIFT Alliance Web Platform
UPI	Unique Product Identifier
UI	User Interface
UTI	Unique Transaction Identifier
XML	Extensible Markup Language

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	Purpose .....	1
1.2	Scope .....	1
<b>2</b>	<b>PARTICIPANT INTERFACE .....</b>	<b>3</b>
2.1	ISO 20022 XML Messages .....	3
2.1.1	Supported ISO 20022 XML Message Types .....	3
2.1.2	Business Application Header (BAH) .....	4
2.1.3	Usage Guidelines .....	4
2.1.4	Submission Approach .....	4
2.1.5	Submission File Format .....	4
2.1.6	Response Approach .....	5
2.1.7	Response File Format .....	5
2.2	Trade Data Submission by Participants .....	7
2.2.1	Supported Asset Classes .....	7
2.2.2	Supported Action Types and Event Types .....	8
2.2.3	Identification of Request File for Trade Data Submissions .....	11
2.2.4	Bulk Submission of Trade Action Requests .....	11
2.2.5	Validation of Trade Action Request .....	12
2.2.6	Request Handling and Response File .....	13
2.3	Valuation Data Submission by Participants .....	15
2.3.1	Supported Action Type .....	15
2.3.2	Identification of Request File for Valuation Data Submissions .....	15
2.3.3	Bulk Submission of Valuation Action Requests .....	16
2.3.4	Validation of Valuation Action Request .....	16
2.3.5	Request Handling and Response File .....	17
2.4	Margin and Collateral Data Submission by Participants .....	19
2.4.1	Supported Action Types .....	19
2.4.2	Identification of Request File for Margin and Collateral Data Submissions .....	19
2.4.3	Bulk Submission of Margin and Collateral Action Requests .....	20
2.4.4	Validation of Margin and Collateral Action Request .....	20
2.4.5	Request Handling and Response File .....	21
2.5	File Submission by Agent .....	23
2.6	Submission Channel .....	24
2.6.1	FileAct Configuration .....	24
2.6.2	FTS Configuration .....	24
2.7	UI Functions .....	26
2.7.1	User Authentication via SWIFT WebAccess .....	26
2.7.2	Internet User Authentication Using SSL Client Certificates .....	26
2.7.3	Client Software/Token Requirements .....	28
2.7.4	URL for UI Functions via Internet .....	28
2.8	Report Collection by Participants .....	29
2.8.1	FTS Configuration Spreadsheet Template .....	29
2.8.2	SWIFTNet FileAct .....	29
2.8.3	SWIFT WebAccess .....	30
<b>3</b>	<b>USE OF SWIFTNET SERVICES .....</b>	<b>31</b>

3.1	SWIFTNet FileAct Service .....	31
3.1.1	Overview of SWIFTNet FileAct Message .....	31
3.1.2	FileAct PDU .....	31
3.2	SWIFT WebAccess Service .....	35
3.2.1	URL and Service Name for TR SWIFT WebAccess Service .....	35
3.2.2	SWIFT User Certificates Set-up .....	35
3.2.3	SWIFT RBAC Role Assignment .....	36
3.2.4	Installation and Configuration of SWIFT Software .....	36
3.2.5	Browser Configuration .....	36
<b>4</b>	<b>FILE SPECIFICATION .....</b>	<b>37</b>
4.1	File Level Reference .....	37
4.2	Action Level Reference .....	38
4.2.1	Trade Action Request Reference .....	38
4.2.2	Valuation Action Request Reference .....	38
4.2.3	Margin and Collateral Action Request Reference .....	39
4.3	Supported Character Set .....	39
4.4	Case Conversion and Case Sensitivity on String Data Fields .....	40
4.5	Parties Information .....	40
4.6	Return Code .....	41

#### **Appendix A – Usage Guidelines (ISO 20022)**

#### **Appendix B – List of Supported Data Elements & Related Validations (ISO 20022)**

#### **Appendix C – Trade Data Model (ISO 20022)**

## 1 INTRODUCTION

### 1.1 Purpose

The purpose of this document is to provide participants of Hong Kong Trade Repository Reporting Service (HKTR) the information required to:

- Access the HKTR system's UI functions through SWIFT WebAccess or Internet;
- Specify the SWIFT environment configuration required to access the HKTR system through SWIFT WebAccess and FileAct service;
- Develop systems where required to provide straight-through processing (STP) between the participant's back-office systems and the HKTR system through various channels provided.

Within each organization of HKTR participants (or simply referred to as "participants" hereafter), the target audience is:

- Developers who develop and support the interface to the HKTR system;
- System administrators who manage the SWIFT environment and its configuration;
- Compliance department;
- Departments responsible for trading and recording OTC derivatives trades; and,
- Those who plan for making system changes to meet the technical requirements of the HKTR system.

Moreover, this document includes the file specifications in ISO 20022 message standard for trade, valuation, margin and collateral information submission by participants.

### 1.2 Scope

This document focuses on the ways to access the HKTR system through different channels. SWIFTNet service description information is also given, in order to support development and configuration of SWIFT solutions. Access to the HKTR system for STP through various channels is covered. Moreover, the participant needs access to the system via SWIFT WebAccess service or Internet, in order to obtain enquiry and report information as well as upload trade data and maintain operational parameters. SWIFT WebAccess and FileAct are standard SWIFTNet services and the details are not addressed in this document.

It is intended that this document should duplicate as little as possible information available from SWIFT. It should be read in conjunction with the standard SWIFT

documentation set, with which the participant is expected to be familiar, in particular the SWIFT User Handbook [1]. Other documents quoted in the Document References are for reference of further details on a specific topic.



## 2 PARTICIPANT INTERFACE

### 2.1 ISO 20022 XML Messages

#### 2.1.1 Supported ISO 20022 XML Message Types

The HKTR system supports the following ISO 20022 XML message types:

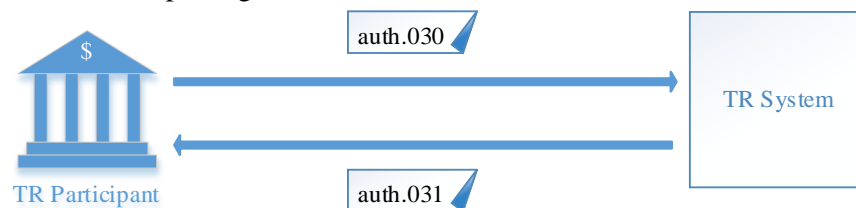
Message Type	ISO 20022 Message Type	Usage
Trade	auth.030	Trade data reporting
Valuation	auth.030	Valuation data reporting
Margin and Collateral	auth.108	Margin and collateral data reporting
Reporting Status Advice	auth.031	Response message return from HKTR system

The following diagram illustrates the workflow of data reporting from the participants based on exchange of ISO 20022 XML messages.

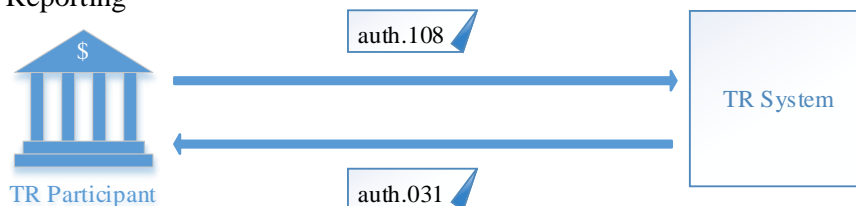
#### Trade Reporting



#### Valuation Reporting



#### Margin and Collateral Reporting



## 2.1.2 Business Application Header (BAH)

For data reporting in ISO 20022 message standard, reporting parties need to provide corresponding header message termed the Business Application Header (BAH). The header message is used together with the ISO 20022 XML message in a request / response file. For the structure of the messages in a request file and response file, refer to section 2.1.5 and section 2.1.7.

The HKTR system supports the following ISO 20022 XML message type for Business Application Header:

Message Type	ISO 20022 Message Type	Usage
Business Application Header	head.001	The header message in request file / response file

## 2.1.3 Usage Guidelines

ISO 20022 Standard sets out an open standard for all possible fields used by worldwide jurisdictions. The data elements to be reported, their associated format, definition and usage in the base message can be further refined according to Hong Kong regulators' requirements. The local guidelines of using the ISO 20022 XML message for local reporting purpose are collectively described in a set of usage guidelines. For details, refer to Appendix A.

Please note that the Usage Guidelines is also accessible via SWIFT MyStandards. Reporting parties are advised to refer to the HKTR Info Page on the registration steps so as to access the most up-to-date information of the Usage Guidelines.

## 2.1.4 Submission Approach

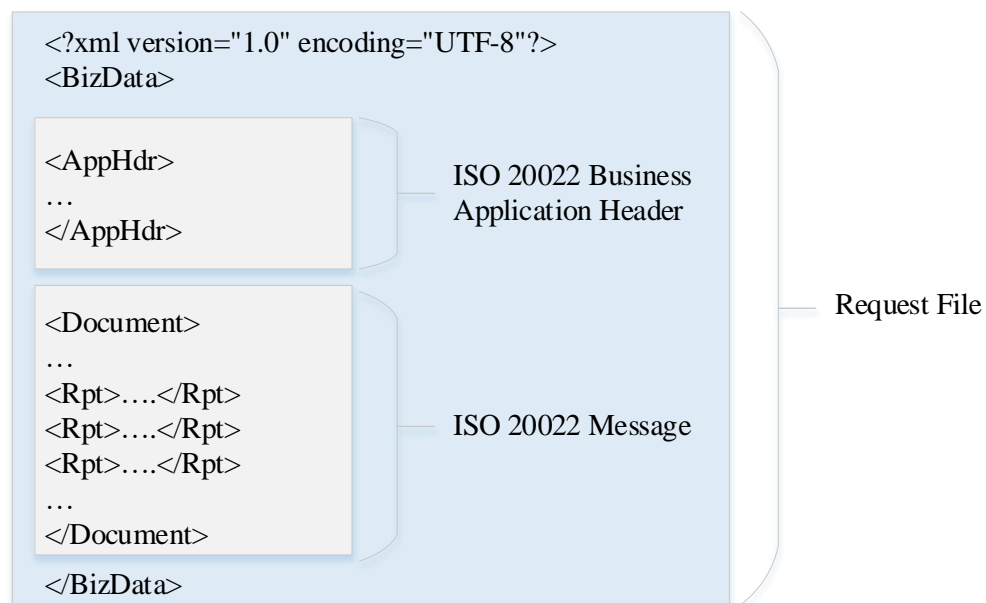
Similar to FpML/CSV based data reporting (before the ISO implementation), HKTR system only supports file-based submission in ISO 20022 data reporting. File-based submission allows participant to specify multiple reporting data records inside a single request file.

To avoid ambiguity of reporting intention, each file can only contains discrete type of trade data containing either trade, valuation or margin and collateral reporting data. In addition, no FpML/CSV based reporting data can be mixed with ISO 20022 messages inside the same file.

## 2.1.5 Submission File Format

In ISO 20022 data reporting, a request file is a XML file which contains one application header and one ISO 20022 message document. The ISO 20022 message document contains one or more reporting data records.

The structure of an ISO 20022 XML request file is illustrated in the diagram below:



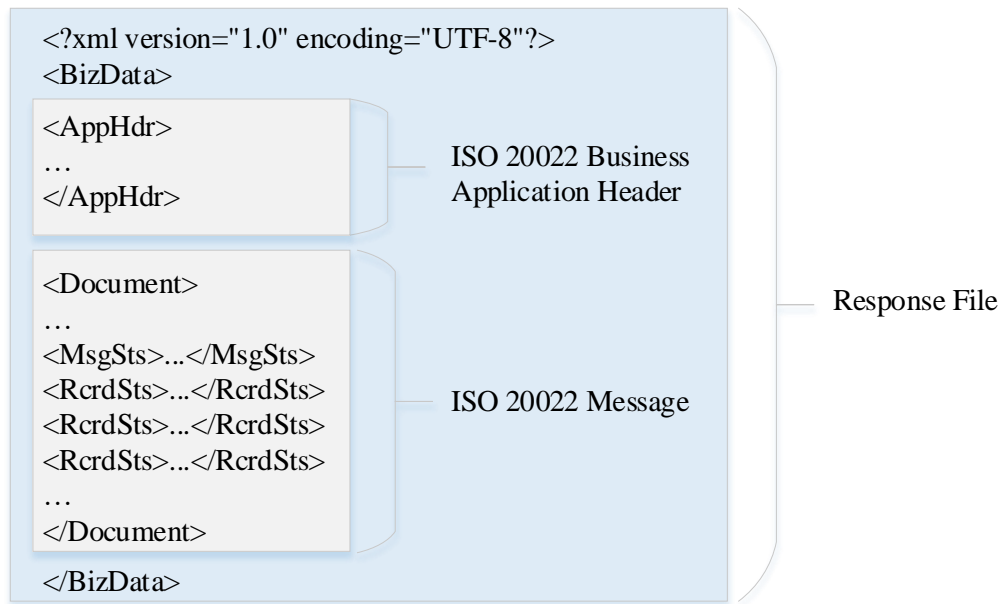
#### 2.1.6 Response Approach

Similar to FpML/CSV based data reporting (before the ISO implementation), HKTR system only supports file-based response message in ISO 20022 data reporting for trade, valuation, margin and collateral.

#### 2.1.7 Response File Format

Similar to request file, a response file is a XML file which contains one application header and one ISO 20022 message document. The ISO 20022 message document contains one or more response message records.

The structure of an ISO 20022 XML response file is illustrated in the diagram below:



## 2.2 Trade Data Submission by Participants

### 2.2.1 Supported Asset Classes

The HKTR system supports the following asset classes in ISO 20022 data reporting:

- Interest Rate
- Currency (Foreign Exchange)
- Commodity
- Equity
- Credit

## 2.2.2 Supported Action Types and Event Types

Action type represents the type of action to be applied to a reported trade transaction. The HKTR system supports the following trade action types:

Action Type	Definition / Description
New (NEWT)	The creation of the first transaction resulting in the generation of a new UTI.
Modify (MODI)	A modification of the terms of a previously reported transaction due to a newly negotiated modification (amendment) or a filling in of not available missing information (e.g., post price transaction). It does not include correction of a previously reported transaction.
Correct (CORR)	A correction of erroneous data of a previously reported transaction.
Terminate (TERM)	A termination of a previously reported transaction.
Error (EROR)	A cancellation of a wrongly submitted entire transaction in case it never came into existence or was not subject to the reporting requirements under the applicable law of a given jurisdiction, or a cancellation of a duplicate report.
Revive (REVI)	An action that reinstates a reported transaction that was reported with action type “Error” or terminated by mistake or expired due to an incorrectly reported Expiration date.
Transfer out (PRTO)	A transfer of a transaction from one reporting agent to another reporting agent (change of reporting agent) or other administration reason such as to stop a reporting agent from further accessing the subsequent trade action of a particular trade.

According to ISO20022 standard, event type indicates what kind of business event is associated with particular OTC derivative contract. The HKTR system supports the following trade event types:

Event Type	Definition / Description
Trade (TRAD)	Creation or modification of a transaction.
Novation/Step-in (NOVA)	A novation or step-in legally moves part or all of the financial risks of a transaction from a transferor to a transferee and has the effect of terminating/modifying the original transaction so that it is either terminated or its notional is modified.
Post trade risk reduction exercise (COMP)	Compressions and other post trade risk reduction exercises generally have the effect either of terminating or modifying (i.e., reducing the notional value) a set of existing transactions and/or of creating a set of new transaction(s). These processes result in largely the same exposure of market risk that existed prior to the event for the counterparty.
Early termination (ETRM)	Termination of an existing transaction prior to expiration date.
Clearing (CLRG)	Central clearing is a process where a central counterparty (CCP) interposes itself between counterparties to transactions, becoming the buyer to every seller and the seller to every buyer and thereby ensuring the performance of open transactions. It has the effect of terminating an existing transaction between the buyer and the seller.
Exercise (EXER)	The full or partial exercise of an option or swaption by one counterparty of the transaction.
Allocation (ALOC)	The process by which portions of a single transaction (or multiple transactions) are allocated to one or multiple different counterparties and reported as new transactions.
Clearing & Allocation (CLAL)	A simultaneous clearing and allocation event in a central counterparty (CCP).
Credit event (CREV)	An event that results in a modification or a termination of a previously submitted credit transaction. Applies only to credit derivatives.
Transfer (PTNG)	The process by which a transaction is transferred to another reporting agent that has the effect of the closing of the transaction reported by one reporting agent and opening of the same transaction using the same UTI by a different agent.
Inclusion in position (INCP)	Inclusion of a CCP-cleared transaction or other fungible transactions into a position, where an existing transaction is terminated and either a new position is created or the notional of an existing position is modified.
Corporate event	The process by which a corporate action is taken on

Event Type	Definition / Description
(CORP)	equity underlying that impacts the transactions on that equity.
Update (UPDT)	Update of an outstanding transaction performed in order to ensure its conformity with the amended reporting requirements.

The following table illustrates the supported combination of “Action Type” and “Event Type”. Rows list all allowable action types and column list all allowable event types. White boxes with a check symbol (✓) indicate if the given combination is allowed and all other combinations are expected to be rejected.

Action type & Event type combinations		Event Type													No Event type required
		Trade (TRAD)	Novation/Step-in (NOVA)	Post trade risk reduction exercise (COMP)	Early termination (ETRM)	Clearing (CLRG)	Exercise (EXER)	Allocation (ALOC)	Credit event (CREV)	Clearing & Allocation (CLAL)	Transfer (PTNG)	Corporate event (CORP)	Update (UPDT)	Inclusion in position (INCP)	
Action Type	New (NEWT)	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	
	Modify (MODI)	✓	✓	✓	✓		✓	✓	✓			✓	✓	✓	✓
	Correct (CORR)														✓
	Terminate (TERM)		✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	
	Error (EROR)														✓
	Revive (REVI)														✓
	Transfer out (PRTO)										✓				



### 2.2.3 Identification of Request File for Trade Data Submissions

The HKTR system mandates the file naming convention to ensure the uniqueness of the files submitted.

The file name is in the following convention:

**treqiso-<participant id>-<generation date>-<user file reference>.xml**

Format String	Description
treqiso	The prefix of request file for trade data reporting in ISO 20022. Must be “treqiso” in lowercase.
<participant id>	HKTR Participant ID (Submitting party). ID in uppercase and lowercase characters will be treated in the same way.
<generation date>	Date of file generation in yyymmdd format
<user file reference>	<p>It is an in-house unique reference assigned by the participant which can be up to a maximum of 35 characters in length. For information of allowable character set on this field, please refer to section 4.3.</p> <p>This user file reference must be the same as the Business Message Identifier quoted in the Business Application Header. Moreover, the two file references must match in a case-sensitive manner.</p>
xml	Only XML file extension is supported in ISO 20022. File extension in uppercase and lowercase characters will be treated in the same way.

Following this naming convention, the participant should generate a unique file name for each request file. The HKTR system supports multiple submissions of files per day for the same participant.

### 2.2.4 Bulk Submission of Trade Action Requests

The HKTR system allows the submission of a trade action request file which contains multiple trade actions. The HKTR system will then process the trade action requests according to their order in the request file for each trade.

To ensure the files correlated to the same trade can be processed in sequence by system, participants should send a new request file after the response file of the previous request file is received.

Please note that each file should contain no more than 125 requests, and that the file size should not be larger than 50M bytes.

## 2.2.5 Validation of Trade Action Request

### 2.2.5.1 Format and Syntax Checking

The HKTR system will firstly validate the file name and file content to ensure the file content integrity and consistency.

The system will then perform schema validations against the business application header (BAH) and the business message for trade reporting (i.e. auth.030). The request file should be formatted correctly according to the request file structure described in section 2.1.5 and conform the usage guidelines described in Appendix A/SWIFT MyStandards. If the message contains fields that are not supported by the system or are not applicable to the corresponding action type of business message, it will be rejected.

A request file will be rejected as a whole if it is not formatted correctly or failure to adhere to the schema requirements of the business application header (BAH).

The schema validation of business message (i.e. auth.030) will be validated in trade action request level. Failure to adhere to the schema requirements of an individual trade action request in a file will not lead to the whole file being rejected.

The system will then perform validations on data elements in both header and business message. It validates the data type, format, allowable values and the business rules associated with each data element.

### 2.2.5.2 Core Business Validation

In addition to format and syntax checking, HKTR system will perform some core business validations during data capture to ensure the business integrity. For example, the system will ensure the targeted trade exists and the status is valid for the post trade actions.

### 2.2.5.3 Unique Reference

Participants are required to specify a unique file reference in the file header for each trade action request file submitted to the HKTR system. Each trade action request must also be assigned with a unique action request reference. Refer to section 4.1 and 4.2 for the exact field names.

### 2.2.5.4 Sequence Checking

For any post trade action received, the HKTR system will process the actions in

chronological order according to their order in the request file for each trade. If there are more than one intra-day post trade actions for the same trade, participants are required to put the post trade actions within the file according to the correct event timestamp sequence.

#### 2.2.5.5 Trade Identifier and its Uniqueness

The Unique Transaction Identifier (UTI) is a mandatory field for trade reporting and is used for trade identification. To ensure proper trade identification, the system will verify its uniqueness of the UTI within the same Entity responsible for reporting.

In cases where some legacy trades could solely be identified by proprietary IDs (such as UTI-USI or UTI-TID) at the UTI data field, the TR system will ensure the uniqueness of the populated value, regardless of the scheme used.

However, the UTI value can be reused when the previously reporting trade carrying the same UTI value in the HKTR has already been Terminated, Transferred out, Errored.

#### 2.2.5.6 Non-amendable Fields.

Below fields are non-amendable fields, the content in these fields should remain unchanged as they were initially submitted to the system. The system will reject the post trade actions if such fields are updated.

- Asset Class
- Execution timestamp
- Entity responsible for reporting
- Unique Transaction Identifier (UTI)

### 2.2.6 Request Handling and Response File

#### 2.2.6.1 Handling of Rejected Request

If validation on a trade action request fails, the HKTR system will reject that request and return the rejection reason in a response file to the submitting participant. As a result, the response file will contain the validation results of individual trade action requests indicating whether they are accepted or rejected by the system.

Rejected trade action requests will not be further processed by the system, and they will not be kept in the HKTR system.

#### 2.2.6.2 Handling of Accepted Request

For a valid trade action request, the HKTR system will proceed to process it according to its action types. Valid trade action requests will be kept in the HKTR system as historical records.

#### 2.2.6.3 Identification of Response File

For every request file submitted to the HKTR system, a response file will be generated and returned to the participant after each trade action request in the request file has been processed.

The response file contains one response record corresponding to each trade action request record. However, when there is exceptional situation in which some response records cannot be properly formatted due to critical errors identified in the trade action request file, the whole request file will be rejected with a file-level response code.

Similar to the request file, the response file in ISO 20022 will be in XML format.

The file name is in the following convention:

**trspiso-<participant id>-<generation date>-<user file reference>-<TR file reference>.xml**

Format String	Description
trspiso	The prefix of response file for trade data reporting in ISO 20022. Must be “trspiso” in lowercase.
<participant id>	HKTR Participant ID. Always in uppercase characters.
<generation date>	Date of file generation in yyymmdd format.
<user file reference>	It is an in-house unique reference assigned by the participant in the request file.
<TR file reference>	It is a unique file reference generated by the HKTR system.
xml	Only XML file extension is supported in ISO 20022. Always in lowercase characters.

## 2.3 Valuation Data Submission by Participants

### 2.3.1 Supported Action Type

The following valuation action is supported by the HKTR system:

Action Type	Definition / Description
Valuation (VALU)	An update of a valuation of a transaction. There will be no corresponding Event type.

The HKTR system supports the reporting of valuation data of a reported trade through the use of valuation action request.

### 2.3.2 Identification of Request File for Valuation Data Submissions

The HKTR system mandates the file naming convention to ensure the uniqueness of the files submitted.

The file name is in the following convention:

**vreqiso-<participant id>-<generation date>-<user file reference>.xxx**

Format String	Description
vreqiso	The prefix of request file for valuation data reporting in ISO 20022. Must be “vreqiso” in lowercase.
<participant id>	HKTR Participant ID (Submitting party). ID in uppercase and lowercase characters will be treated in the same way.
<generation date>	Date of file generation in yyyyymmdd format
<user file reference>	It is an in-house unique reference assigned by the participant which can be up to a maximum of 35 characters in length. For information of allowable character set on this field, please refer to section 4.3.  This user file reference must be the same as the Business Message Identifier quoted in the Business Application Header. Moreover, the two file references must match in a case-sensitive manner.
xml	Only XML file extension is supported in ISO 20022. File extension in uppercase and lowercase characters will be treated in the same way.

Following this naming convention, the participant should generate a unique file name for each request file. The HKTR system supports multiple submissions of files per day for the same participant.

### 2.3.3 Bulk Submission of Valuation Action Requests

Like trade action request submissions, the HKTR system allows the submission of a valuation request file which contains multiple valuation action requests. The HKTR system will then process the valuation action requests according to their order in the request file.

Like trade action request submissions, there are limits on the file size and the number of action requests can be contained inside a file. Each valuation request file should contain no more than 2500 action requests, and that the file size should not be larger than 50M bytes.

### 2.3.4 Validation of Valuation Action Request

#### 2.3.4.1 Format and Syntax Checking

Similar to validating trade action request file, the HKTR system will firstly validate the file name and file content to ensure the file content integrity and consistency.

The system will then perform schema validations against the business application header (BAH) and the business message for valuation reporting (i.e. auth.030). The request file should be formatted correctly according to the request file structure described in section 2.1.5 and conform the usage guidelines described in Appendix A/SWIFT MyStandards. If the message contains fields that are not supported by the system or are not applicable to the corresponding action type of business message, it will be rejected.

A request file will be rejected as a whole if it is not formatted correctly or failure to adhere to the schema requirements of the business application header (BAH).

The schema validation of business message (i.e. auth.030) will be validated in valuation action request level. Failure to adhere to the schema requirements of an individual valuation action request in a file will not lead to the whole file being rejected.

The system will then perform validations on data elements in both header and business message. It validates the data type, format, allowable values and the business rules associated with each data element.

#### 2.3.4.2 Core Business Validation

In addition to format and syntax checking, HKTR system will perform some core business validations during data capture to ensure the business integrity. For example, the system will ensure the targeted trade exists and the status is valid for the valuation actions.

#### 2.3.4.3 Unique Reference

Participants are required to specify a unique file reference in the file header for each valuation action request file submitted to the HKTR system. Each valuation action request must also be assigned with a unique action request reference. Refer to section 4.1 and 4.2 for the exact field names.

#### 2.3.4.4 Correlation of Trade and Valuation Data

A valuation request correlates the trade it wants to operate on using either a Unique Transaction Identifier or a Unique Transaction Identifier associated with a TR Trade Reference, and then updates its valuation record according to the specified valuation date.

#### 2.3.5 Request Handling and Response File

##### 2.3.5.1 Handling of Rejected Request

Similar to trade action request processing, if validation on a valuation action request fails, the HKTR system will reject that request and return the rejection reason in a response file to the submitting participant. As a result, the response file will contain the validation results of individual valuation action requests indicating whether they are accepted or rejected by the system.

Rejected valuation action requests will not be further processed by the system, and they will not be kept in the HKTR system.

##### 2.3.5.2 Handling of Accepted Request

For a valid valuation action request, the HKTR system will proceed to process it and it will be kept in the HKTR system.

##### 2.3.5.3 Identification of Response File

For every request file submitted to the HKTR system, a response file will be generated and returned to the participant after each valuation action request in the request file has been processed.

The response file contains one response record corresponding to each valuation action request record. However, when there is exceptional situation in which some response records cannot be properly formatted due to critical errors identified in the valuation action request file, the whole request file will be rejected with a file-level response code.

Similar to the request file, the response file in ISO 20022 will be in XML format.

The file name is in the following convention:

**vrspiso-<participant id>-<generation date>-<user file reference>-<TR file reference>.xml**

Format String	Description
vrspiso	The prefix of response file for valuation data reporting in ISO 20022. Must be “vrspiso” in lowercase.
<participant id>	HKTR Participant ID. Always in uppercase characters.
<generation date>	Date of file generation in yyyyMMdd format.
<user file reference>	It is an in-house unique reference assigned by the participant in the request file.
<TR file reference>	It is a unique file reference generated by the HKTR system.
xml	Only XML file extension is supported in ISO 20022. Always in lowercase characters.



## 2.4 Margin and Collateral Data Submission by Participants

### 2.4.1 Supported Action Types

The following margin and collateral actions are supported by the HKTR system:

Action Type	Definition / Description
Collateral or Margin update (MARU)	An update to collateral margin data. There will be no corresponding Event type.
Correct (CORR)	A correction of erroneous data of a previously reported collateral or margin data.

The HKTR system supports the reporting of margin and collateral data through the use of margin and collateral action requests.

### 2.4.2 Identification of Request File for Margin and Collateral Data Submissions

The HKTR system mandates the file naming convention to ensure the uniqueness of the files submitted.

The file name is in the following convention:

**mreqiso-<participant id>-<generation date>-<user file reference>.xxx**

Format String	Description
mreqiso	The prefix of request file for margin and collateral data reporting in ISO 20022. Must be “mreqiso” in lowercase.
<participant id>	HKTR Participant ID (Submitting party). ID in uppercase and lowercase characters will be treated in the same way.
<generation date>	Date of file generation in yyyyMMdd format
<user file reference>	It is an in-house unique reference assigned by the participant which can be up to a maximum of 35 characters in length. For information of allowable character set on this field, please refer to section 4.3.  This user file reference must be the same as the Business Message Identifier quoted in the Business Application Header. Moreover, the two file references must match in a case-sensitive manner.
xml	Only XML file extension is supported in ISO 20022. File extension in uppercase and lowercase characters will be treated in the same way.

Following this naming convention, the participant should generate a unique file

name for each request file. The HKTR system supports multiple submissions of files per day for the same participant.

#### 2.4.3 Bulk Submission of Margin and Collateral Action Requests

Like trade action request submissions, the HKTR system allows the submission of a margin and collateral request file which contains multiple margin and collateral action requests. The HKTR system will then process the margin and collateral action requests according to their order in the request file.

Like trade action request submissions, there are limits on the file size and the number of action requests can be contained inside a file. Each margin and collateral request file should contain no more than 2500 action requests, and that the file size should not be larger than 50M bytes.

#### 2.4.4 Validation of Margin and Collateral Action Request

##### 2.4.4.1 Format and Syntax Checking

Similar to validating trade action request file, the HKTR system will firstly validate the file name and file content to ensure the file content integrity and consistency.

The system will then perform schema validations against the business application header (BAH) and the business message for margin and collateral reporting (i.e. auth.108). The request file should be formatted correctly according to the request file structure described in section 2.1.5 and conform the usage guidelines described in Appendix A/SWIFT MyStandards. If the message contains fields that are not supported by the system or are not applicable to the corresponding action type of business message, it will be rejected.

A request file will be rejected as a whole if it is not formatted correctly or failure to adhere to the schema requirements of the business application header (BAH).

The schema validation of business message (i.e. auth.108) will be validated in margin and collateral action request level. Failure to adhere to the schema requirements of an individual margin and collateral action request in a file will not lead to the whole file being rejected.

The system will then perform validations on data elements in both header and business message. It validates the data type, format, allowable values and the business rules associated with each data element.

#### 2.4.4.2 Core Business Validation

In addition to format and syntax checking, HKTR system will perform some core business validations during data capture to ensure the business integrity. For example, the system will check if the Collateral timestamp is a future timestamp.

#### 2.4.4.3 Unique Reference

Participants are required to specify a unique file reference in the file header for each margin and collateral request file submitted to the HKTR system. Each margin and collateral action request must also be assigned with a unique action request reference. Refer to section 4.1 and 4.2 for the exact field names.

#### 2.4.5 Request Handling and Response File

##### 2.4.5.1 Handling of Rejected Request

Similar to trade action request processing, if validation on a margin and collateral action request fails, the HKTR system will reject that request and return the rejection reason in a response file to the submitting participant. As a result, the response file will contain the validation results of individual margin and collateral action requests indicating whether they are accepted or rejected by the system.

Rejected margin and collateral action requests will not be further processed by the system, and they will not be kept in the HKTR system.

##### 2.4.5.2 Handling of Accepted Request

For a valid margin and collateral action request, the HKTR system will proceed to process it and it will be kept in the HKTR system.

##### 2.4.5.3 Identification of Response File

For every request file submitted to the HKTR system, a response file will be generated and returned to the participant after each margin and collateral action request in the request file has been processed.

The response file contains one response record corresponding to each margin and collateral action request record. However, when there is exceptional situation in which some response records cannot be properly formatted due to critical errors identified in the margin and collateral action request file, the whole request file will be rejected with a file-level response code.

Similar to the request file, the response file in ISO 20022 will be in XML format.

The file name is in the following convention:

**mrspiso-<participant id>-<generation date>-<user file reference>-<TR file reference>.xml**

Format String	Description
mrspiso	The prefix of response file for margin and collateral data reporting in ISO 20022. Must be “mrspiso” in lowercase.
<participant id>	HKTR Participant ID. Always in uppercase characters.
<generation date>	Date of file generation in yyymmdd format.
<user file reference>	It is an in-house unique reference assigned by the participant in the request file.
<TR file reference>	It is a unique file reference generated by the HKTR system.
xml	Only XML file extension is supported in ISO 20022. Always in lowercase characters.

## 2.5 File Submission by Agent

An Agent can submit the trade action / valuation action / margin and collateral action request files on behalf of a participant.

In ISO 20022 data reporting, an agent relationship is defined per asset class instead of per sub product. There is a separate agent relationship configuration section for ISO 20022 in the participant maintenance function.

Upon the receipt of a request file from an Agent, the HKTR system will check whether the submitting party is authorized to submit the request file on behalf of the corresponding reporting parties for that asset class. If not, the HKTR system will reject the request file. This applied to trade and valuation reporting.

As margin and collateral data on portfolio basis associated with more than one transactions which are belonging to multiple asset classes. Therefore, different from valuation, an agent can submit the margin and collateral data for reporting parties whenever the agent is authorized to submit the trade data of any asset class through any selected channel for the party.

Under the current phase, the agent relationship is maintained by HKMA only, according to the information provided by HKTR participants. When reporting parties intends to switch agent of an asset class for trade and valuation reporting, it is necessary to notify HKTR in advance.

## 2.6 Submission Channel

The HKTR system provides a UI function for participants to upload the trade action requests, valuation action requests and margin and collateral action requests in files according to the published standards.

Alternatively, participants can submit the request files to the HKTR system through the File Transfer Service (“FTS”) on ICLNet or FileAct on SWIFTNet. The subscription of FTS and FileAct service are provided by HKICL and SWIFT respectively.

In summary, the HKTR system supports the following 3 methods of data submission by participants.

- FTS on ICLNet
- FileAct on SWIFTNet
- UI Upload

For the first two methods, the HKTR system requires participants to configure specific parameters through the UI function prior to data submission and report collection. Please refer to the following subsections for more details.

### 2.6.1 FileAct Configuration

Configuration is required for the following parameter:

- SWIFT FileAct Distinguished Name (DN) – the DN applicable to the participant’s submitting data via SWIFTNet FileAct. Multiple FileAct DNs may be configured by participants for use in the HKTR system.

The parameter can be viewed and maintained by participants using the View/Maintain Participant Details UI functions. Please refer to the User Manual [\[3\]](#) for the details of the UI functions.

### 2.6.2 FTS Configuration

For FTS, Connect:Direct software with Secure+ feature is used by participants to submit trade action / valuation action / margin and collateral action requests and receive reports. The data will be carried across ICLNet, which provides reliable and secure network.

Many financial institutions in Hong Kong are currently using the FTS on ICLNet for various purposes. New FTS users are required to contact HKICL for the subscription of the service and the arrangement of the necessary testing and set-up.

For the submission of trade action / valuation action / margin and collateral action request files, the participant's Connect:Direct server is required to initiate a Connect:Direct process to the FTS server hosted by HKICL. Participants have to provide the following information for the file transfer process:

<b>Argument</b>	<b>Description</b>
File Name	The file name of the request file.
Connect:Direct Process Name	The process name to be provided by HKICL that will handle the file transfer.
HKTR Notification Shell Script	The shell script name of HKTR system to be provided by HKICL that will process the trade action / valuation action / margin and collateral action request file.

Participants can optionally define a job in its Connect:Direct server, which will invoke a job to process the response files returned by HKICL.

A spreadsheet template will be distributed to the participants for their inputs of FTS configurations for response files such as Output File Path, Output File Name and Batch Job to be triggered at participants' servers.

## 2.7 UI Functions

Participant users can use online functions provided by the HKTR system via the following means:

- SWIFT WebAccess service (requiring prior login to SWIFT network through SWIFT Alliance Web Platform (AWP) / Personal Token)
- Internet

### 2.7.1 User Authentication via SWIFT WebAccess

Different from GUI function access through Internet as described in section 2.7.2, user authentication is not entirely done by HKTR application but integrated with SWIFT's central authentication service. While SWIFT users authenticate themselves to log in SWIFT network, the users have the convenience to use the same credentials and similar SWIFT user interface to log in HKTR application.

When a SWIFT user logs in HKTR system via SWIFT WebAccess service by accessing the application URL over SWIFT WebAccess, the user is presented with a SWIFT WebAccess login screen (rather than HKTR system's application login interface in the case of Internet channel). After submitting the password of the SWIFT user, SWIFT will authenticate the user on behalf of HKTR system and pass SWIFT's user ID to HKTR system for identification purpose if the authentication is successful.

When the SWIFT user ID is passed to the HKTR system for login purpose, the HKTR system needs to associate the SWIFT user ID with corresponding application user ID. If the association has yet been made, a SWIFT User Account Association web page will be invoked for the user to associate the currently used SWIFT user with HKTR application user profile. The participant ID, application user ID and application user password will be required in order to activate such association.

Once the association between SWIFT's user and HKTR system's application user profile is established, the function will no longer be prompted for subsequent login of that user.

The SWIFT user account association can be viewed in the View User Account UI function. The association can be removed using the Maintain User Account UI function, if necessary.

### 2.7.2 Internet User Authentication Using SSL Client Certificates

Participant users that access the HKTR system via the Internet are required to be authenticated when logging in using an SSL Client certificate (digital certificate). This is configured through the Maintain User Account UI function provided by the HKTR



system. The URL associated with the access through Internet is the same one used for connecting to the primary or DR site.

At the time of user login, in addition to entering the user's Participant ID, User Name and Password, the user's SSL certificate is retrieved and forwarded to the HKTR system with the logon request. The login screen allows the user to select a certificate from the browser's certificate repository.

The credentials of the user's certificate are validated as follows:

- The user's certificate is checked for expiry;
- The certificate must be signed by a Certification Authority (CA) that is designated as a trusted CA by HKICL;
- The certificate is checked against the consolidated list of revoked certificates maintained for the HKTR system.

If this validation fails, the login request is rejected. The HKTR system will ensure that the SSL Client certificate associated with the user account can be shared within own participant but not shared between different participants during user account maintenance. The certificate revocation lists for the agreed CAs are maintained in the HKTR system and are updated periodically.

Digital certificate issued by the following authorized CAs will be supported by the HKTR system:

i) Local Certification Authority:

- Digi-Sign Certification Services Limited ("Digi-Sign")
- Hongkong Post

ii) Global Certification Authority:

- Geotrust
- Verisign<sup>1</sup>
- Symantec<sup>2</sup>
- Entrust
- IdenTrust
- DigiCert

Please note that the list of CAs above is not finalized and subject to change in future.

---

<sup>1</sup> Security Business of Verisign has been acquired by Symantec in 2010.

<sup>2</sup> Security Business of Symantec has been acquired by DigiCert in 2017.

### 2.7.3 Client Software/Token Requirements

For accessing to the HKTR system for UI functions via SWIFT WebAccess service:

- SWIFT Alliance Web Platform (AWP) / Personal Token (refer to SWIFT's manuals for more details)
- AWP / Personal Token supported Windows versions
- AWP / Personal Token supported Browser versions

For accessing UI functions of the HKTR system under Windows 10 and Window 11 platform:

- Google Chrome version 130
- Microsoft Edge version 130

### 2.7.4 URL for UI Functions via Internet

The HKTR system implementation provides a browser-based user interface through Internet for enquiry, report viewing and administrative functions.

The URLs available to participants are as follows:

URL	IP Address	Purpose
<a href="https://tr.cmu.org.hk/tr/login">https://tr.cmu.org.hk/tr/login</a>	Production: 113.28.158.73 (primary) 118.143.124.9 (backup) 107.162.133.234 (contingency)  Disaster Recovery: 113.28.158.74 (primary) 118.143.124.10 (backup) 107.162.133.234 (contingency)	Production and Disaster recovery site
<a href="https://truat.cmu.org.hk/tr/mem/login">https://truat.cmu.org.hk/tr/mem/login</a>	118.143.124.8 (primary) 107.162.133.232 (contingency)	Member test
<a href="https://truat.cmu.org.hk/tr/sim/login">https://truat.cmu.org.hk/tr/sim/login</a>	118.143.124.8 (primary) 107.162.133.232 (contingency)	Simulation test

## 2.8 Report Collection by Participants

The reports generated by the HKTR system are broadly classified into the following three types:

- (1) System reports – Reports are generated in off-line batch mode at pre-defined time or after a specific event, in PDF format (for administrative functions reports) or CSV format (for trade / valuation / margin and collateral related reports), and can be delivered via file transfer or viewed/downloaded via UI function;
- (2) Enquiry-Initiated User Requested reports – Reports are generated in background mode, in PDF (for administrative functions reports). Users can check report generation status, view or download the generated report via the View Report List function; and
- (3) UI Enquiry reports – Reports that are tied to the enquiry functions. The report shows the real-time enquiry result. Reports generated are sent to the browser front-end for user's viewing. The user can then save the report or print it out. Saved enquiry results are in CSV format.

The following channels are supported by the HKTR system:

- FTS on ICLNet
- FileAct on SWIFTNet
- Browser retrieval - through UI functions

The means of browser retrieval is always available by default. For system reports with multiple report formats, each report format can be configured to be delivered via FTS and/or FileAct as the additional delivery channel.

Depending on the report type of system reports, the delivery channel can be configured on a participant basis using Maintain Report Schedule UI function.

### 2.8.1 FTS Configuration Spreadsheet Template

A spreadsheet template will be distributed to the participants for their inputs of FTS configurations for each system report such as Output File Path, Output File Name and Batch Job to be triggered at participants' servers.

### 2.8.2 SWIFTNet FileAct

For the configuration information required for reports received through SWIFTNet FileAct service, refer to section 2.6.1 for details.

### 2.8.3 SWIFT WebAccess

The HKTR system provides functions for users to browse reports in PDF file format. Users should ensure that their PC workstations are installed with the necessary client software for viewing PDF files.

For the configuration information required to use SWIFT WebAccess service, refer to section 3.2 for details.

### 3 USE OF SWIFTNET SERVICES

#### 3.1 SWIFTNet FileAct Service

SWIFTNet FileAct is used as one of the channels for the participants to submit trade information to the HKTR system and/or receive response files/reports generated by the HKTR system. The specific SWIFTNet FileAct messaging implementation used is Store-and-Forward.

##### 3.1.1 Overview of SWIFTNet FileAct Message

The SWIFTNet FileAct message is composed of two components – (i) a Protocol Data Units (PDU) header which contains addressing information and a cryptographic element used to authenticate the message, and (ii) a payload containing the actual file content.

##### 3.1.2 FileAct PDU

The FileAct PDU contains addressing information, additional service-specific information such as non-repudiation, and any authentication information for the message.

Note that only the UTF-8 encoding scheme is supported for SWIFTNet FileAct XML messages.

SWIFTNet addressing in the FileAct PDU is derived from the Request Type, Sender Distinguished Name (DN), Receiver DN, and SWIFTNet Service name.

The PDU message structure and the permitted values for parameters are described as follows:

Element name	Permitted Values
Saa:DataPDU	
Saa:Revision	
Saa:Header	
Saa:Message	
Saa: MessageIdentifier	refer to section 3.1.2.1
Saa: Sender	
Saa: DN	refer to section 3.1.2.2
Saa: Receiver	
Saa: DN	refer to section 3.1.2.2
Saa: NetworkInfo	
Saa:Service	refer to section 3.1.2.3
Saa: FileLogicalName	refer to section 2.2.3 (for trade) or 2.3.2 (for valuation) or 2.4.2 (for margin and collateral) .

### 3.1.2.1 Request Types for SWIFTNet Service

The Request Type for HKTR system's FileAct service is "demt.001". This is validated by SWIFT and the HKTR system.

### 3.1.2.2 SWIFTNet Sender and Receiver Addressing

The following table defines the Sender and Receiver DN to be used for the HKTR system.

For an overview of how Sender and Receiver addressing works in the context of SWIFTNet, refer to [1.2].

Sender DN	Receiver DN	Purpose
Any of the production participant DNs configured within the HKTR system.	ou=tr,o=hkikhkh,o=swift	Production
Any of the pilot participant DNs configured within the HKTR system.	cn=trsimtest,ou=test,o=hkikhkh,o=swift	Simulation test (Note 1)
Any of the pilot participant DNs configured within the HKTR system.	cn=trmemtest,ou=test,o=hkikhkh,o=swift	Member test (Note 2)

Note:

1. Simulation test is to allow participants to get familiar with the operations of the HKTR system on an end-to-end basis under a production-like testing environment.
2. Member test is for those participants to test their straight-through processing (STP) interfaces to the HKTR system.

### 3.1.2.3 SWIFTNet FileAct Service Name

Two separate services are respectively defined to facilitate provisioning of FileAct and WebAccess services at SWIFT.

For SWIFTNet FileAct service, the service of HKTR system is shared with eMBT/eCMT system, that is, the SWIFT's Closed User Group (CUG) of HKTR system is the same as eMBT/eCMT system. Service subscription is required if participants have not subscribed eMBT/eCMT's SWIFTNet FileAct service.

SWIFTNet FileAct services are available in the pilot and production environments of HKTR system.

SWIFTNet FileAct Service Name	Service Description	SWIFTNet Environment	Purpose
hkicl.rtgs.fileact	Hong Kong RTGS Store-n-Forward FileAct Service (Live)	Production (Live service)	FileAct Production
hkicl.rtgs.fileact!p	Hong Kong RTGS Store-n-Forward FileAct Service (Pilot)	Production (Pilot service)	FileAct Member Test and Simulation Test

For SWIFT WebAccess URL and service name, refer to section 3.2.1.

#### 3.1.2.4 Additional Information Contained in the PDU

SWIFTNet Non-Repudiation feature is not supported by the HKTR system, and the following rule applies:

Element Name	Usage
Saa:DataPDU	
Saa:Header	
Saa:Message	
Saa:SecurityInfo	
Saa:SWIFTNetSecurityInfo	
Saa:IsNRRequested	Not allowed to be set. If set, the message is rejected by SWIFT.

SWIFTNet Copy feature for FileAct is not supported by the HKTR system, and the following rule applies:

Element Name	Usage
Saa:DataPDU	
Saa:Header	
Saa:Message	
Saa:NetworkInfo	
Saa:SWIFTNetNetworkInfo	
Saa:IsCopyRequested	Not allowed to be set. If set, the message is rejected by SWIFT.

The possible duplicate emission indicator specified in the PDU is ignored by HKTR system.

### 3.1.2.5 FileAct Signature

Messages are authenticated using the SNL cryptographic protocols as implemented using the SignatureList. The SwSec:Signature element contains a number of elements, used in FileAct requests as follows:

Element Name	Permitted Values
SwSec:Signature	
SwSec:KeyInfo	
SwSec:SignDN	SWIFTNet FileAct DN configured by participants in HKTR system. Refer to section 2.6.1 for details.



## 3.2 SWIFT WebAccess Service

Before a SWIFT user can access HKTR system's GUI function through SWIFT network over SWIFT WebAccess service, the administrator and security officer must go through a set of SWIFT configurations on network connectivity, security and software configurations.

The following sub-sections within section 3.2 provide the high level description of SWIFT WebAccess configurations. For more detailed information, refer to SWIFT's related manuals or contact respective account manager of SWIFT.

### 3.2.1 URL and Service Name for TR SWIFT WebAccess Service

Different from SWIFTNet FileAct service, which is common to both HKTR and eMBT/eCMT systems, the SWIFT WebAccess service for HKTR system and eMBT/eCMT system are two individual SWIFT services. There is an individual Closed User Group (CUG) for HKTR system, service subscription of TR SWIFT WebAccess service is mandatory for all HKTR participants.

The service names and URLs of the SWIFT WebAccess services for Live and Pilot environments are listed as follows for WebAccess service subscription and configuration:

SWIFT WebAccess Service Name	URL	IP Address	SWIFTNet Environment	Purpose
hkicl.tr.gui	https://hkicl-tr.browse.swiftnet.sipn.swift.com/tr/login	149.134.1.184	Production (Live service)	Production and Disaster recovery site
hkicl.tr.gui!p4	https://hkicl-tr-pilot-memtest.browse.swiftnet.sipn.swift.com/tr/mem/login	149.134.1.176	Production (Pilot service)	Member test
hkicl.tr.gui!p5	https://hkicl-tr-pilot-simtest.browse.swiftnet.sipn.swift.com/tr/sim/login	149.134.1.177	Production (Pilot service)	Simulation test

For information on SWIFT WebAccess, refer to the SWIFTNet Service Description in [1.1].

### 3.2.2 SWIFT User Certificates Set-up

Each SWIFT user must have a unique SWIFT certificate from SWIFT to associate with one unique application user profile predefined in HKTR system. User cannot associate the same SWIFT user certificate with more than one application user profile in HKTR system.

### 3.2.3 SWIFT RBAC Role Assignment

In order for a SWIFT user to pass through SWIFT's role based access control before successfully logging in HKTR system, each SWIFT user must be assigned to one default RBAC role "access\_to\_service" for TR SWIFT WebAccess Service by participant's security officer.

### 3.2.4 Installation and Configuration of SWIFT Software

Before a SWIFT user can log in HKTR system the user should log in SWIFT WebAccess environment first. To achieve SWIFT WebAccess environment login, the following ways are provided by SWIFT:

- SWIFT Alliance Web Platform (AWP)
- Personal Token

For the participants who access HKTR system's WebAccess service using AWP, the latest WebAccess GUI package version should be installed.

For the participants / users who access HKTR system's WebAccess service using Personal Token, appropriate token installation software should be installed.

For more detail, refer to SWIFT's documentation [\[2\]](#)

### 3.2.5 Browser Configuration

For the details of browser configuration for SWIFT Alliance Web Platform (AWP) or Personal Token in SWIFT WebAccess, refer to SWIFT's documentation [2].

## 4 FILE SPECIFICATION

As mentioned in previous section, the trade / valuation / margin and collateral action requests are in ISO 20022 XML format and submitted to HKTR through a file. For every request file submitted to HKTR system, a response file will be generated and returned to the participant via its originating submission channel. The response files are also in ISO 20022 XML format, which would contain the processing results of action requests.

Refer to Appendix A/SWIFT MyStandards, B and C for the usage guidelines of ISO 20022 XML, list of supported data elements & related validations and trade data model respectively.

### 4.1 File Level Reference

Participants are required to specify a unique file reference<sup>3</sup> in the field called “Business Message Identifier” under Business Application Header (BAH) for each of their trade / valuation / margin and collateral action request files submitted to the HKTR system. This file reference will then be included in “Message Report Identifier” of the response file, allowing participants to correlate the response file with the corresponding submitted file. Additionally, the HKTR system will assign its own unique TR file reference in the “Business Message Identifier” under Business Application Header (BAH) and filename for each response file returned to the participants.

The following is the data element name and its XML path of the file level reference:

	ISO 20022 Message Type	Data Element Name	XML path of file reference	Origin of the reference
<b>Request</b>	head.001	Business Message Identifier	/AppHdr/BizMsgIdr	Assigned by submitting parties
<b>Response</b>	head.001	Business Message Identifier	/AppHdr/BizMsgIdr	Unique TR file reference generated by the system
<b>Response</b>	auth.031	Message Report Identifier	/Document/FinInstrmRptgStsAdvc/StsAdvc/MsgRptIdr	The original “Business Message Identifier” under head.001 of the request file

---

<sup>3</sup> The HKTR system only requires the file reference to be unique either within all submitted trade action request files or within all submitted valuation action request files or within all submitted margin and collateral action request files. File references are allowed to be duplicated across these three types of files. In return, the HKTR file reference generated in the response will also be unique either within all trade action response files or within all valuation action response files or within all margin and collateral action response files.

## 4.2 Action Level Reference

Similar to the File Level Reference, each action request and response includes a Technical Record Identification that correlates the request with the response of the action request.

The following subsections show the data element name and its corresponding XML path for each type of action level reference:

### 4.2.1 Trade Action Request Reference

	ISO 20022 Message Type	Data Element Name	XML path of file reference	Origin of the reference
<b>Request</b>	auth.030	Technical Record Identification	/Document/DerivsTradRpt/TradData/Rpt/\$actionType/TechAttribts/TechRcrdId	Assigned by reporting parties
<b>Response</b>	auth.031	Original Record Identification	/Document/FinInstrmRptgStsAdvcs/StsAdvcs/RcrdSts/OriginalRcrdId	The original “Technical Record Identification” of corresponding record under auth.030 of the request file

### 4.2.2 Valuation Action Request Reference

	ISO 20022 Message Type	Data Element Name	XML path of file reference	Origin of the reference
<b>Request</b>	auth.030	Technical Record Identification	/Document/DerivsTradRpt/TradData/Rpt/\$actionType/TechAttribts/TechRcrdId	Assigned by reporting parties
<b>Response</b>	auth.031	Original Record Identification	/Document/FinInstrmRptgStsAdvcs/StsAdvcs/RcrdSts/OriginalRcrdId	The original “Technical Record Identification” of corresponding record under auth.030 of the request file

#### 4.2.3 Margin and Collateral Action Request Reference

	ISO 20022 Message Type	Data Element Name	XML path of file reference	Origin of the reference
<b>Request</b>	auth.108	Technical Record Identification	/Document/DerivsTradMrgnDataRpt/TradeData/Rpt/\$actionType/TechAttrbts/TechRcdId	Assigned by reporting parties
<b>Response</b>	auth.031	Original Record Identification	/Document/FinInstrmRptgStsAdvcs/StsAdvcs/RcdSts/OriginalRcdId	The original “Technical Record Identification” of corresponding record under auth.108 of the request file

#### 4.3 Supported Character Set

Participants need to encode OTC derivative data into ISO 20022 XML format in UTF-8 subject to the following limited character set for different data fields:

Data Fields	Available character sets	Unicode Code Point
File Reference (Business Message Identifier)	Alphanumeric characters and underscore, i.e. ‘A’ to ‘Z’, ‘a’ to ‘z’, ‘0’ to ‘9’ and ‘_’.	0030 – 0039, 0041 – 005A, 005F, 0061 – 007A
Technical Record Identification	Alphanumeric characters, hyphen, underscore and colon, i.e. ‘A’ to ‘Z’, ‘a’ to ‘z’, ‘0’ to ‘9’, ‘-’, ‘_’ and ‘:’.	002D, 0030 – 003A, 0041 – 005A, 005F, 0061 – 007A
Party ID - HKTR Entity ID, Party ID - SWIFTBIC	Alphanumeric characters, i.e. ‘A’ to ‘Z’, ‘a’ to ‘z’, ‘0’ to ‘9’	0030 – 0039, 0041 – 005A, 0061 – 007A
Remarks 1- 13 (in “supplementary data” message block)	Basic Latin including English alphabets, numbers and symbols, Carriage Return (CR) and Line Feed (LF) characters, Latin-1 supplement including Cent sign, Pound sign, Yen sign and German, Latin-Extended-A including French	000A, 000D, 0020 – 007E, 00A0 – 00FF, 0100 – 017F
Other fields	Basic Latin including English alphabets, numbers and symbols.  The character set of each field may be further restricted. For details, refer to Usage Guidelines.	0020 – 007E

#### 4.4 Case Conversion and Case Sensitivity on String Data Fields

Upon receiving a trade / valuation / margin and collateral action request, the following string fields will be converted to uppercase characters before further processing (e.g. trade correlation, validations and uniqueness checking, etc) and then stored in the system.

Asset Class(es)	Field(s) that are transformed and processed in uppercase characters by the system
All	Party ID - Legal Entity Identifier [LEI], Party ID - SWIFTBIC code [SWIFTBIC], Party ID - Unique Business Identifier [UBIN], Party ID - Number of the Certificate of Incorporation (CI) (for locally incorporated companies)/Certificate of Registration (CR) (for companies incorporated overseas) [CICR], Party ID - Business Registration Number (BRN) [BRNO], Party ID - User Defined Code [USDC], Party ID - Natural Persons [NATURAL PERSONS], Party ID - TR Entity ID [TRID]

For string fields not listed in the above table, e.g. file references, business message identifiers, trade references, action references, technical record identifications, unique transaction identifiers or Collateral portfolio codes, these field values will remain undistorted in the system, and will be processed *case-sensitively*.

#### 4.5 Parties Information

Where an OTC derivative transaction is reported to the HKTR system, the report should reflect three types of parties as following:

1. *Submitting Party* means the party who submits the transaction (either trade, valuation or margin and collateral action request) to the HKTR system.
2. *Entity responsible for reporting* means the party who has the reporting obligation to report the transaction.
3. *Counterparty 1/2* are the contracting parties of the trade being reported.

#### 4.6 Return Code

Upon the receipt of a request, the HKTR system returns either a normal response message indicating that the processing result is successful, or an error message in case of rejection. The error message can carry up to 20 Return Codes with the corresponding descriptions of rejection(s), depending on the type of errors.

For details of the validation rules and return codes, refer to Appendix B.