RMA – Best Practise - 2022

White paper

Note:

The Payments Market Practice Group (PMPG) is an independent body of payments subject matter experts from Asia Pacific, EMEA and North America. The mission of the PMPG is to:

- Take stock of payments market practices across regions
- Discuss, explain, and document market practice issues, including possible commercial impact
- Recommend market practices, covering end-to-end transactions
- Propose best practice, business responsibilities and rules, message flows, consistent implementation of ISO messaging standards and exception definitions
- Ensure publication of recommended best practices
- Recommend payments market practices in response to changing compliance requirements

The PMPG provides a truly global forum to drive better market practices, which, together with correct use of standards, will help in achieving full STP and improved customer service.

Table of Contents

1 Executive Summary

This document has been created to outline the changes that will take place in order to move and maintain Relationship Management within a Centralised Global Platform and support both FIN and FINplus traffic. To improve the Relationship Management process there will be a move to granular relationships based on Business Profiles. This document will outline the processes that will be carried out by SWIFT and required by Financial Institutions in order to move to this new RMA Functionality and the Central Portal.

2 RMA – Supporting the Migration to ISO 200 22

SWIFT migrate Payments-related messages to ISO 20022 standard from Nov 2022. There will be a co-existence period between 2022 to 2025, which will allow sending and receiving of both, MT FIN and ISO XML format messages during that time.

Once CBPR+/SWIFT migrate to ISO 20022 in Nov 2022, every Institution must have the ability to receive MT and ISO (XML) format message (or multi-format message ISO (XML) with embedded MT). This means that by Nov 2022 RMAs must be in place for both the MT and the ISO equivalent messages that can be sent across the network.

To enable the sending and receiving of the ISO 2022 messages, SWIFT will create the ISO equivalent RMA's for the Financial institutions. The process of creating the RMA's for the SWIFT.finplus.InterAct services will be called "bootstrapping". The bootstrapped authorisations will be created within the Central RMA Database by SWIFT..

As a second step Business Profiles will be introduced to replace the current RMA's that are in place. These business profiles will provide granularity and context to the business relationship held between two parties.

3 Bootstrapping

To prevent Institutions from having to create FINplus payment relationships with their counterparties before the ISO 20022 migration in Nov 2022, SWIFT will perform a bootstrapping exercise, which will involve creating FINplus RMAs within the Central database, based on the existing FIN relationships. The Bootstrapping process will ensure that the FINplus authorisations will be "enriched" with the additional request types (see table I section 3.2) if they are already put in place and there will be no impact to the FIN RMA records.

Each Institution is responsible for its RMAs and must validate the FINPlus relationships that SWIFT have created based on current records maintained decentralized by the individual parties. Institutions can use the reporting functionality accessible on the portal which will outline all central relationship records. Institutions have the opportunity to validate, create or revoke any authorisations via the local RMA interface.

It should be noted that it will be possible to create locally issued authorisations with additional granularity levels as long as they adheres to the consistency check and FIN and FINPlus are kept synchronized.

Only the messages types in scope of CBPR+ with backward compatibility (using in-flow translation or Transaction Manger will be bootstrapped.

3.1 Payments related bootstrapping

The FINplus RMA's in the table below will be created as part of bootstrapping. Where a *Blanket RMA is in place, then all FINplus message types within the below table will be set up as part of bootstrapping.

3.2 RMA creation within the Bootstrapping exercise

If authorised in FIN	FINplus Created in Bootstrapping exercise
MT103	pacs.008 pacs.004 pacs.002
MT192/292	camt.056
MT196/296	camt.029
MT202/205	pacs.009 pacs.004 pacs.002
MT199/299	pacs.002
MT210	camt.057

4 "9" Series equivalent camt messages

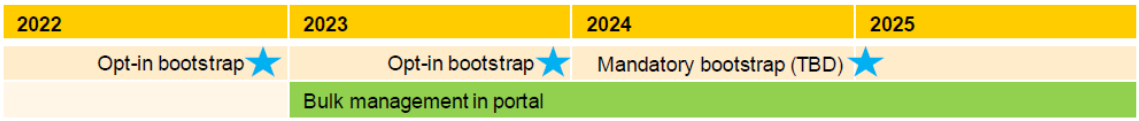
Today, there is no RMA required in order to send an MT 9xx series statement or advice to a counterparty. . FINplus requires a RMA in place of any messages, including all camt messages, the MT Cat 9 equivalent.

In order to facilitate Institutions having camt reporting RMAs in place, SWIFT will monitor the FIN MT Statement and Advice traffic received into an institution over a period of 7 months (December 2021 – June 2022 and provide optional bootstrapping for the camt. equivalents on an authorisation to receive basis.

If authorised in FIN	FINplus Created in Bootstrapping exercise
MT941, MT942	camt.052
MT940, MT950	camt.053
MT900, MT910	camt.054

There are 3 opportunities to utilise bootstrapping for camt messages.

*Blanket RMA's are where an RMA is set up between two parties to permit the sending of any message. This is unlike RMA Plus which is the more granular version and allows the message types permitted to be stipulated.



One opportunity to include camt in the distribution file required a formal request by the end of May 2022.

For those institutions not ready to receive Statements and Advices in camt. Format yet, SWIFT will repeat the bootstrap exercise following the process above at the end of 2023.

A decision will be made together with the industry whether a further bootstrapping is required in 2025before the retiring of the FIN messages in November 2025

4.1 Sending Mass Requests via the Central Portal

At the beginning of 2023 SWIFT will publish documentation on a Mass Authorisation functionality that will be available within the Central Portal.

The concept of the Mass Authorisation functionality will permit Institutions to carry out the following:-

1. Select a modification they want to perform (this can include the statement and advising RMA's - camt.052,053,054)
2. Select their BIC
3. Select the list of counterparties
4. Confirm

Once the Institutions confirm, the application will go over all the relationships that fit the criteria and add the chosen message (in this case camt.xxx) to the existing authorization (or create a new one) if not yet present. The Central Platform will send out a corresponding RMA message to a counterparty for each authorization, as it would have been if individually issued. This will allow any institution to indicate their readiness with a single action to all counterparties, but can also be used for any other type of activity (like mass revocation during cleanup, or add a new business flow to a list of existing counterparties.)

5 Pain.001 relay, pain.002 relay, pacs.010 & camt.060

Only messages in scope for the Nov 22 migration that also have In-flow translation available, are included within the bootstrapping exercise. This means that there are some message which will not included within the bootstrapping. Such RMA's will need to be set up manually.

For more information on this please see the connectivity guidance paper which lays out the migration principles :
https://www2.swift.com/knowledgecentre/publications/s_pltfm_s_pltfm_evo_conn_guid/2.0

6 Actions associated to Bootstrapping

6.1 July 2022 - Action

The Bootstrapping will occur on the 30th July 2022.

Institutions can import the distribution file which will update all of their FINplus RMA's onto their RMA Interface.

Once imported Institutions can then adjust their authorisations where needed using their local RMA Interface.

From the 20th November 2022 any newly created FINplus RMA's will become active.

When creating or updating a relationship the authorisation must always be created on both FIN and FINplus channels.

RMA's that are issued locally will only update within the Central Portal if consistency is kept between FIN and FINplus. This means that there must be the message type equivalence, the Status and the validity period all matching in order for the RMA to be set up centrally, otherwise the inconsistent set of authorisations will be aborted and must be re-issued.

7 Technical Consistency Checks

Once the bootstrapping exercise is completed (30th July 2022), SWIFT will ensure consistency between the RMAs that are set up for FIN and FINplus.

The consistency check will monitor that the locally issued RMA authorisations match the status and validity period across the FIN and FINplus requests. Local requests will be held for 15 minutes to ensure that they are received for both channels.

The following attributes must match in order for the synchronization to be consistent.

- Status (authorised, revoked, rejected)
- Validity period
- Key request Types

The consistency checks will be limited to the following messages

FIN (inbound)	FINplus (Inbound)
MT103	Pacs.008, pacs.004, pacs.002
MT202	Pacs.009, pacs.004, pacs.002

It is important to set up the FINplus equivalent of a FIN based on the fact that there are now dedicated messages in ISO 20022 for certain business practices. For example, previously an RMA for an MT103 would cater for an MT103, MT103 Return message and an MT103 Reject message. In FINplus the equivalent messages will need to be set up which would be pacs.008, pacs.004 and pacs.002 to accommodate the previous use cases for the FIN MT103.

If an Institution fails to issue a consistent set of authorisations then the authorization will be aborted back to the issuer where they must be re-issued.

Note that if an Institution fails to issue a consistent set of authorisations then it is important to issue a new set as soon as possible. When the authorization is aborted, the issuers RMA records will be de-synchronised with the central and correspondents RMA database.

8 The evolution to the Business Profile

In many cases, "Blanket" RMA's were set up between Institutions which permitted them to send any message type. This gives no granularity and provides no information concerning the Business Relationship that is held between the two parties. In order to foster the adoption of RMA granularity and ease the cross protocol consistency requirements, the concept of "business profiles" has been introduced. A business profile groups different message types that support a given business flow and will ensure that only the traffic that supports the business relationship is authorised.

They also allow to provide additional business context to an otherwise technical authorisation.

Business profiles will be used when creating authorisations from the central portal. A Business Profile will ensure that only the traffic that supports the business relationship is authorised.

All existing FIN and FINplus message types are covered by a business profile:-

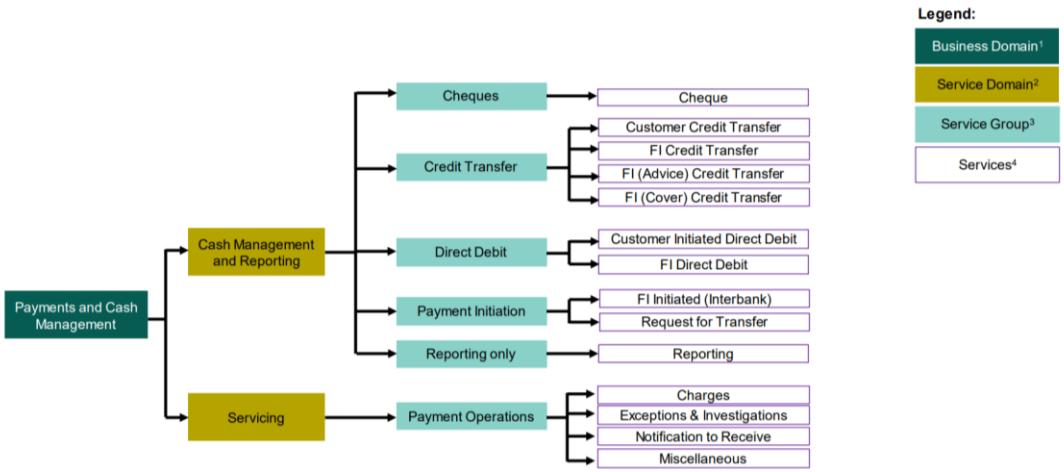
- Payments and Cash Management
- Securities
- Trade Services
- Foreign Exchange (Treasury Markets)
- Travellers Cheque
- Market Infrastructure Service

There are several layers within a Business Profile and they are described as follows:-

- Business Domain – Business domains define a coherent collection of capacities within the broader business area. (In the BIAN Service Landscape the business domains are associated with skills and knowledge recognizable in the banking business.)
- Service Domain – is the finest level of partitioning, each defining unique and discrete business capacities. The Service Domains are the 'elemental building blocks' of a service landscape.
- Service Group - Collection of related service capabilities
- Services - Collection of granular services.

An example of these levels:

Payments and Cash Managements



For a full list of Business Profiles that have been defined, please go to the knowledge Centre page: https://www2.swift.com/knowledgecentre/kb_articles/5024789 and see the "RMA_Profiles" attachment to that page.

9 The Relationship Management Portal

9.1 Current Functionality

The following functionality is currently available within the Central Portal:-

9.1.1 Search for Authorisations

From the home page of the Relationship Management Portal you can use a Basic search by BIC or an advanced search option which will permit operators to search for an authorization based on multiple attributes such as their own BIC and/or Country, or a Counterparties BIC and/or Country, the Authorisation Service, Direction, Status, Start date or End date.

9.1.2 Review your Search Results

The results of your search can be provided back to you within a comprehensive search results page. The view within this page allows an operator to use filters within the search results page to further refine their search/results criteria.

9.1.3 Review your Authorisation Details Page

This page will display to the operator the status of the authorisations between their Institution and their Correspondent. During the migration phase this information can be used to ensure that authorisations exist for incoming and outgoing traffic to send and receive both FIN and the equivalent FINplus messages.

There are three Statuses for Authorisations:

- Authorised
  - Receive traffic – You have granted your correspondent the authorization to send traffic to your institution.
  - Send traffic – Your counterparty has granted your institution the authorization to send them traffic

- Partially authorised – This status is only available during the migration period. It means your relationship status for FIN and FINplus are not aligned.
- Not authorised – Receive traffic not authorised or Send traffic not authorised. Receive traffic not authorised: Your institution did not grant an authorization to the counter party to send you traffic, your instiutution has revoked the authorization, the counterparty refused the authorization or the authorization has expired. Send traffic not authorised: The counterparty did not grant your institution an authorization to send them traffic, the counterparty has revoked the authorization, you refused an authorization granted by the counterparty, or the authorisation has expired.

9.1.4 Reports

You can create Reports of authorisations based on chosen report criteria. It is possible to then select certain criteria to be included into the output of the report.

9.1.5 Distribution Files

You can create distribution files in XML format to import Relationship Management records into another application. The distribution file can be created manually or you can automate the distribution of the file. For more information regarding the File structure please visit the following location:https://www2.swift.com/knowledgecentre/publications/rma_serv_7_0_op_guid/5.0?topic=ref_120917.htm It is important to note that Central RMA distribution files must be used only to synchronise messaging interfaces or back-office applications but never to overwrite the data in a local RMA interface (The exception to this is the FINplus bootstrap).

9.2 Upcoming Functionality – available in an upcoming release in the Q3 2022

9.2.1 4-Eye Check

It is possible to set up 4-eye checks within the RMA Portal if required

9.2.2 The "To do" page

The to do page will display all of the actions required against authorisations. It can be used to manage any outstanding actions required. It can also be utilised to invoke "to do" items against users where a 4-eye check is required/invoked. It is possible to filter on the "to do" page by BIC or by Action required. The only action that can be taken in the "to do" page is to mark an action as Read. Once you have marked a notification as read/completed it will remove it from the "to do" list display.

9.2.3 Communications – Exchange Queries and Answers with Correspondents

It will be possible to send and receive query and answers about a business relationship with a counterparty in that relationship. It will be also possible to search for queries and answers easily using search criteria. You can view and create communications in two different ways:

1. On the **Communications** page available in the main menu, you can view communications with all correspondents. Unread communications are flagged.
2. On the details page for a specific authorisation, you can send messages and view the communication history between your BIC and your correspondent.

Individuals that manage relationships at the receiving institution can then read these messages and reply to them. The big advantage of this mechanism is that the message reaches the appropriate personnel within the institution that deal with correspondent relationships and that the query and

answer trace can be kept of the entire conversation and can be stored together with the authorization.

9.2.4 Manage your authorization to receive traffic

An authorization to receive traffic is the authorization that your BIC grants to a correspondent BIC to enable them to send messages to you. The following actions will be available on the authorization to receive traffic:

- Grant (create)
- Modify
- Revoke

9.2.5 Manage authorisations to send

An authorization to send means that the counterparty granted your BIC an authorization to send them traffic. After you activate the authorization, it will have the status of "Authorised" and your BIC will be allowed to send traffic to that counterparty. The following actions will be available on the authorisation to send:

- Activate
- Refuse

9.2.6 View previous authorisations

It will be possible to view all previous authorisations to receive and to send, that you have agreed with your correspondents.

9.2.7 Event Log

It will be possible to view the history for an authorisation within the event log. All of the actions related to the authorisation will be logged.

10 RMA Evolution Timeline

October 2021	Relationship Management Portal Pilot available
April 2022	Mass subscription to the portal by SWIFT of all connected BIC's
July 2022	Bootstrap for FINplus Technical Consistency Check
Q3 2022	Relationship Management features will be released on the Relationship Management Portal in Pilot and Live
November 2022	CBPR+ General Availability
December 2023 (tentative)	SWIFT will no longer support Customers Local RMA Interfaces

11 Subscribe to the Relationship Manager Portal

Every customer receives automatic access to the central RMA portal to extract central authorization information (reporting and distribution files). RMA management functionalities will become optionally available towards the end of 2022, activation details will be shared by SWIFT in Q3 2022

12 Observations and Recommendations from the PMPG Market Practice Guidelines for the adoption of the RMA Best Practice document, Version 6, published in December 2020

Within the published paper for the RMA Best Practice there were some observations and recommendations made. Comments have been added into the table from the document to show where the Relationship Management Portal will meet some of these expectations and ease the pain points of others:-

	Observations	**Recommendations**	**Relationship Management Portal**
1	When an RMA request is initiated it may sit in a queue that may not be checked or is checked infrequently.	1) The RMA request queue should be reviewed on a daily basis. In line with SWIFT documentation, an acknowledgement should be sent for any RMA request received within 48 hours. 2) However, it should be recognised that KYC and due diligence requirements need to be met before an RMA can be fully accepted. It is the choice of the receiving entity as to what action to take and what to respond with. Example acknowledgement – *We have received your RMA request to exchange SWIFT messages with our organisation. Please note that this is request is subject to internal review and due diligence. Please monitor your queues for additional correspondence if required.* More details on the SWIFT documentation can be found here:	1) The Central Relationship Management Portal will ensure that the Counterparty will now always receive requests. There will no longer be a technical barrier as there will be only one single database. This will eliminate delays and issues. 2) The "technical barrier" disappears that is introduced by the store and forward mechanism (where updates are not consumed at all or late). With everyone working on the same database, the restrictions can be immediately enforced while still giving full control on the sending side. when the scope gets expanded (so more message types are allowed) : Any increase in scope, as today will require an approval before the authorization to send becomes active. This means indeed that the sender can activate and accept. However when the scope gets reduced (so less message types are allowed) : any decrease in scope, the central portal will

			automatically activate as the issuer requires immediate protection, this also means that sending applications that get synchronized from the central database will automatically receive any scope reductions (without the need to accept them)
2	Due diligence needs to be undertaken when an RMA request is received. This can be onerous and time-consuming.	1) An organisation determines their own controls and due diligence procedures. Where possible existing industry tools and available information should be leveraged to support any due diligence. e.g. SWIFT KYC Registry tool, attestations to the SWIFT CSP, …	In an End state within the Relationship Management Portal all of the KCY information and Self Cert information will sit in the central portal (this will be introduced from about 2024) This will help to significantly improve the experience. Discussions on this functionality and the timing for implementation will be determined by the Institutions and the priority given for enhancements as per feedback from the relevant industry working group.
		2) When an RMA request is initiated the receiving entity may follow up with due diligence questions that may include KYC and CSP. The organization requesting the RMA should be prepared for follow up messages and respond in a timely manner.	There will be no technical barriers anymore within the Central Relationship Management Portal. There will be an indication as to when a receiver has seen your request (if both are on the central portal)
3	Often the recipient does not know the reason for the RMA request or who to contact at the sending organisation. Finding contact details can be difficult.	1) The requesting organisation should send an additional message to support the RMA request providing the reason for the request and if possible, a contact at the sender. This will aid in cases where additional information is required. Example – *Please see our RMA request to exchange SWIFT messages between our organisations dated 22nd Feb 2020. This request is to support commercial payment activity for transfers due to your customers. Please contact Mary.Smith(at)exampleemail.com for further details if required.*	There will be a future offering to provide internal or external notes attached to the authorization regarding context and details and contact details. Institutions will be able to register their RMA Administrators within the Portal so that they can receive notifications (via email for example). However this functionality is TBC as to when this future improvement will be implemented. This may not be of use as the RMA Administrator and the Business owner will be different people. To be discussed further with the possibility to allow to identify "business" owners within the portal who can provide input on their domain.
		2) Where appropriate, organisations may identify RMA owners for specific message types within their own internal controls and procedures. This ensures understanding of the business requirements for that particular type of request.	Within the Central Relationship Management Portal there will be Business profiles – these can be aligned to business owners within the Institutions. They provide the Business context of the relationship. A possible solution being considered is to allow to register these business owners within the portal linked to a given domain. This could then be made

			internally/externally available depending on preferences.
		3) At the time of publication, RMA requests for FINPlus messages should be limited to specific business reasons and where the recipient is aware of the requirement for the FINPlus RMA exchange. Blanket requests for FINPlus messages to mirror existing RMA exchanges should **not** be attempted at this time. Note: this best practice paper will be updated as the FINPlus service matures.	The concept of the Blanket request will be phased out due to the use of Business Profiles which are granular
4	Lack of RMA product awareness within organisations can mean that setting up and maintaining an RMA is problematic. This is particularly noticeable with the use of RMA+.	1) Organisations internal processes and procedures should be based on SWIFT usage guides. 2) The RMA+ utility is free of charge and allows organisations greater control on their SWIFT messaging exchanges. Please note that both the sending and receiving organisations do not both need to use RMA+.	Today there is often a big gap between the business discussions and the technical implementation of that discussion. The goal of the portal and use of business profiles is to bridge this gap. The end goal is that an RMA relationship results naturally from the business discussion and that the business discussion can use the business profile handbook as support.
5	An organisation's procedures may revoke all RMAs for a group when this has not been requested	1) An organisation's revocation procedures should account for both the BIC 8 and BIC 4 level. A blanket removal of BICs within a group should not be performed unless there is the appropriate rationale.	There is no mitigating control over this – This is down to individual Institutions behavior. As Business profiles improve the process this should no longer be as much of an issue.
6	RMA Dormancy and relationship management procedures are inconsistent across the industry	1) SWIFT members should make use of the guidance provided by SWIFT on maintaining RMA relationships and ensuring they are up to date - https://www2.swift.com/go/book/bookext052450 This guidance describes the link to the CSP but in particular section "2.11A RMA Business Controls" provides the advice SWIFT gives on existing relationship handling	If KYC and CSP information is available within the Relationship Management Portal, then this would provide guidance / indication against which counterparties you wanted to continue to do business with. Dormancy will be looked at later but it is really up to Institutions to do this themselves. SWIFT should not be revoking RMA's and making a call whether something is dormant or not however there will be tools available within the Relationship Management Portal that will make this easier to manage – for example the Mass revocation functionality.