

GUIDELINES OF ESTABLISHING RMA WITH KDPW IN SEPARATED FUNCTIONAL AREAS (ISO 20022)**CONTENTS**

I	GENERAL	1
II	ESTABLISHING RMA WITH KDPW	1
II.1.	PRODUCTION ENVIRONMENT	1
II.2.	TEST ENVIRONMENT	2
III	ENVELOPE FORMAT	2
IV	BUSINESS APPLICATION HEADER	2

I GENERAL

This document presents the guidelines drafted by Krajowy Depozyt Papierów Wartościowych (KDPW) concerning the SWIFT Relationship Management Application (RMA) which include RMA guidance for KDPW participants as well as other intermediaries concerning ISO 20022 messages dedicated to separate functional areas.

SWIFT RMA is a message security feature enabling the members of the SWIFT network to exchange messages over the network in a controlled fashion. The use of RMA is mandatory for sending and receiving SWIFT FINplus messages.

KDPW expects intermediaries who are not KDPW participants to initiate an RMA Authorisation exchange for SWIFTNet FINplus.

Intermediaries who are KDPW participants and file in a declaration to receive via SWIFT messages dedicated to separate functional areas (declaration available at <https://www.kdpw.pl/uploads/attachments/swift3-en.docx>) should initiate an RMA Authorisation exchange for SWIFTNet FINplus with KDPW immediately after completing the declaration.

KDPW will accept KDPW participants and other intermediaries RMA Authorizations within 24 hours.

II ESTABLISHING RMA WITH KDPW

RMA Authorizations for test and live usage can be exchanged before SWIFTNet FINplus is fully available, as the authorizations are exchanged using dedicated SWIFTNet services 'swift.rma' (live RMA) and 'swift.rma !p' (test RMA).

II.1. Production environment

Please send your live RMA Authorization for service 'swift.finplus' to the SWIFTNet Responder DN "o=kdpwplpw,o=swift", BIC code KDPWPLPW. KDPW will accept and reciprocate upon message reception.

II.2. Test environment

Should you wish to establish test traffic with KDPW for ISO 20022 messages in separate functional areas, you will need to set up RMA Authorizations for the test service in SWIFT FINplus. If so, please send your test RMA Authorization for service 'swift.finplus!pc' to the SWIFTNet Responder DN "o=kdpwplpw,o=swift", BIC code KDPWPLPW. We will accept and reciprocate upon message reception. Note that the BIC-8 used is the live BIC-8.

III ENVELOPE FORMAT

The exact details of the outer envelope used to transmit messages onto SWIFTNet services will depend on the particular software used, but the following elements will always be part of it:

XPath field reference	Value
DataPDU/Header/Message/SenderReference	Message reference to identify this message instance
DataPDU/Header/Message/MessageIdentifier	ISO20022 Message type
DataPDU/Header/Message/Sender/DN	The SWIFTNet Requestor DN of your institution in three levels, e.g. "ou=xxx,o=bankplpw,o=swift"
DataPDU/Header/Message/Receiver/DN	Always "ou=xxx,o=kdpwplpw,o=swift" for communicating with KDPW
DataPDU/Header/Message/NetworkInfo/Service	One of the following values: "swift.finplus" (for live traffic), "swift.finplus!pc" (for test)
DataPDU/Body/AppHdr/	Business Application Header, as described below

These XPath elements are specific to SWIFTAlliance Access. Your system may use a different syntax. Please consult the system documentation.

IV BUSINESS APPLICATION HEADER

Business Application Header (BAH) is standardised by SWIFT. The current version is V02 (head.001.01.02). The minimum BAH content is presented below:

XPath field reference	XPath field reference
AppHdr/Fr/FIId/FinInstId/BICFI	Your institution's live BIC11
AppHdr/To/FIId/FinInstId/BICFI	Always "KDPWPLPWXXX"
AppHdr/BizMsgIdr	Unique message identifier
AppHdr/MsgDefIdr	ISO 20022 message type
AppHdr/CreDt	Message creation date and time including time zone

KDPW uses live BICs in the Business Application Header also in tests and expects live BICs to be used in incoming messages.