

ARM APPLICATION - USER MANUAL

Table of Contents

I INTRODUCTION..... 2

I.1. DEFINITIONS: 2

I.2. ACCOUNT REGISTRATION IN THE SERVICE PORTAL 3

I.3. REQUESTING ACCESS TO THE ARM APPLICATION 3

I.4. REVOCATION OF THE AUTHORIZATION OF THE PERSON WHO HAS ACCESS TO THE ARM APPLICATION..... 4

II LOGGING IN TO THE ARM APPLICATION..... 4

III FUNCTIONALITIES OF THE ARM APPLICATION 5

III.1. TRANSACTIONS 5

III.2. INVOICE ANALYTICS 6

III.3. XML MESSAGES..... 6

III.4. REQUEST HISTORY 7

I Introduction

The document describes the way of applying for access to the ARM U2A channel, the mechanism of obtaining the access and contains user manual for the U2A graphic interface of the system.

I.1. Definitions:

- **Service administrator within an institution** – a user having right to administer requests for access to the of other entity users
- **Permission administrator** – is a person authorized by a participant who is a direct participant in the CSD of the KDPW to manage access to applications in which this participant has or will in the future have a relationship with the KDPW, which, on the date of granting the authorization, are assigned by the KDPW to the appropriate group of services for the type of participation, among which is the ARM service
- **ARM application** - IT system (graphic interface of the U2A channel), used as part of the service provided by KDPW, enabling manual exchange of information through messages between the participant and KDPW
- **Access application** - an application enabling access to the KDPW system through Single Sign On (SSO), available on the KDPW website
- **Message** - form of submitting and receiving information between a participant and KDPW in line with the MiFIR Regulations provisions
- **User account** - an account created by a natural person (user) in the access application
- **User** – a natural person who has an account in the KDPW access application, having the possibility to request an access to the ARM application as a User or Administrator on behalf of an entity that is a participant in the ARM service
- **Service user** - a user who has access to the ARM application on behalf of an ARM participant
- **Rules of access** – „Rules of access to the IT systems of KDPW” define the rules of access and authorization in the KDPW applications dedicated to electronic communication with KDPW and the rules required to set up a system connection with the KDPW applications
- **ARM Rules** – determine the legal basis for KDPW to provide services with respect to collecting and storing data, in accordance with the provisions of MiFIR Regulation
- **Participant** – an entity which is a party to a participation agreement concluded under the KDPW service rules or a party to another agreement concluded in accordance with the service rules or an entity which gains access to other functionalities provided by KDPW
- **ARM service** - a service provided by KDPW (Approved Reporting Mechanism).

I.2. Account registration in the Service Portal

To access the applications available through the Service Portal <https://online.kdpw.pl>, you need to open an access account and download the KDPW Group Authenticator application to a mobile device. The application is used to authenticate application users in the multi-factor authentication (MFA) mechanism implemented in the Service Portal. The application can be downloaded for free from authorised shops: Google Play (Android), App Store (iOS - Apple), and its use is only permitted on phones with unbroken security of the operating systems of these manufacturers. For detailed information please refer to the [Access Account User's Manual: Access Account](#).

By using the same attributes, it is also possible to access the test environments of the services available in the Service Portal: TST <https://tst-online.kdpw.pl> and EDU <https://edu-online.kdpw.pl>.

I.3. Requesting access to the ARM application

Obtaining access to the ARM application requires having the authority to act within the service on behalf of the relevant entity. To do so, it is necessary to apply for access to the application in the role of the:

- User
- Service Administrator - the participant is required to authorize at least one person to act on its behalf in the application in the role of service administrator. This requirement does not apply if the ARM service participant is also a direct participant in the KDPW CSD. In that case, the management of access to the application is carried out through the permission administrator, established in accordance with the contract for direct participation in the KDPW.

After submitting a request for access to the application, it is necessary to provide the KDPW with a statement from the entity, confirming the details of the person submitting the application and his authorization to act in the ARM application. Providing a statement to the KDPW is not required if access is granted by a service administrator authorized by the participant (applies to applications for a user role) or a permission administrator (applies to applications for user and service administrator roles).

Below there are the Instructions for requesting access to the applications provided in the <https://online.kdpw.pl>:

- Submitting a request for access to the application - instructions for KDPW direct participants and issuers at KDPW, entities required to appoint a permission administrator [link](#)
- Submitting a request for access to the application - instruction for entities which are not KDPW direct participants or issuers at KDPW, entities which are not required to appoint a permission administrator [link](#)

I.4. Revocation of the authorization of the person who has access to the ARM application

Access to the application may be revoked:

- by a permission administrator or a service administrator authorised by the participant, directly in the Service Portal online.kdpw.pl,
- where there is no administrator, by KDPW on the basis of the entity's statement concerning the revocation of the authorisation (template below).

Revocation of authorisation - only for users who do not manage application access through a permission administrator - [template](#)

Revocation of authorisation - only for KDPW direct participants and issuers who manage application access through a permission administrator - [template](#)

II Logging in to the ARM application

To sign in to the application, the ARM participant visits the production application [website](#), a page is launched, on which the user is asked to provide login and password as shown below. For test environments the web addresses are <https://tst-online.kdpw.pl> (environment, which is used to test new functionalities) or <https://edu-online.kdpw.pl> (environment with the same configuration as production one).



Sign in

Please sign in to the system to use KDPW Group services

Email Address

Password [Forgot your password?](#)

Sign in



Don't have an account? [Sign up now](#)

PL | EN



After successful sign in the main application screen is entered as shown below:

Choose one of your services

 <p>Trade Repository (EMIR)</p> <p>Transaction Reporting</p>	 <p>Trade Repository (SFTR)</p> <p>Transaction Reporting</p>	 <p>ARM approved reporting mechanism</p> <p>Transaction Reporting</p>	 <p>Manage permissions</p> <p>Administrator</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------

III Functionalities of the ARM application

After clicking the "ARM approved reporting mechanism" tile the following menu opens:

RT19 RT19 Member	Reports							Refresh	New Report
	Transaction Id	Supervis...	Transaction Dat...	Notification type	ISIN	Receiving date	Status		
Reports	<input type="text"/>		yyyy-MM-dd		<input type="text"/>	yyyy-MM-dd			
\$ Statement of fees	+ 7152791	KNF	2021-12-17	NEWT New report	PLHOLWD00017	2021-12-17 12:21:04	Sent to NCA	...	
	+ 7152791	KNF	2021-12-17	NEWT New report	PLHOLWD00017	2021-12-17 12:09:44	Error	...	
</> XML Messages	+ 0241151755	KNF	2021-12-16	NEWT New report		2021-12-16 16:16:04	Sent to NCA	...	
	+ 024115175	KNF	2021-12-16	NEWT New report		2021-12-16 16:02:43	Error	...	
🕒 Request history	+ 024115175	KNF	2021-12-16	NEWT New report		2021-12-16 15:20:52	Sent to NCA	...	

The user can select functionalities from the menu on the left. Clicking the relevant tab redirects to the pages.

III.1. Transactions

The tab shows the transaction reports submitted by a participant on its own and on behalf of the entities represented by the participant. It is possible to filter the records of tab by the following criteria:

- Transaction ID,
- Transaction date,
- Notification type,
- ISIN,
- Receiving date,
- Status.

After finding the requested data, the user can view the item details that have been sent to the KDPW. To do this, click on the + sign to see the details.

a) It is also possible to manually enter transaction data and build a report that will be sent to the NCA. To do this, in the reports tab, click on the button: [New Report](#), which is located in the upper right corner of the screen. Then the user manually enters all the required transaction data and after checking its completeness, approves the report.

New report

1 Report definition 2 Buyer - Account Owner 3 Buyer - Decision Maker 4 Seller - Account Owner 5 Seller - Decision Maker 6 Transaction Details 7 Financial Instrument

Report details

Action Type

Event Date UTC

Transaction Id

Investment Institution ☐ Yes ☐ No

In the event of a need to correct an error or report a similar transaction to the existing one, a convenient option is "copy". The option is available after clicking on the symbol below for the copied transaction:

Reports

[Refresh](#)
[New Report](#)

Transaction Id	Supervis...	Transaction Dat...	Notification type	ISIN	Receiving date	Status	
<input type="text"/>		<input type="text" value="yyyy-MM-dd"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="yyyy-MM-dd"/>	<input type="text"/>	
+ 7152791	KNF	2021-12-17	NEWT New raport	PLHOLWD00017	2021-12-17 12:21:04	✕ Sent to NCA	⋮
+ 7152791	KNF	2021-12-17	NEWT New raport	PLHOLWD00017	2021-12-17 12:09:44	ⓘ Error	📋 Copy
+ 0241151755	KNF	2021-12-16	NEWT New raport		2021-12-16 16:16:04	✕ Sent to NCA	...

Once selected, the transaction data will be copied to the form. It is possible to edit them to remove errors or to enter other data.

III.2. Invoice analytics

Selecting Statement of fees from the menu and selecting the appropriate dates for a given billing period (from-to) allows you to download details of fees for the participant submitting the reports. Data is displayed in a window, but it is also possible to download data to xlsx format.

My desktop

Trade Repository (SFTR)

ARM approved reporting mechanism

Authorization

RT20

RT20

Member

+

Statement of fees

Period (from - to):

May 2021

December 2021

Refresh

Download

Reporting LEI

Member payment

Member count

Reports payment

Reports count

Total payment

Payment with CAP

CAP saving

2021-05-01 - 2021-05-31

259400BASIA000000043

500.00

1

15.40

385

515.40

515.40 PLN

0.00

total:

500.00

1

15.40

385

515.40

515.40 PLN

0.00

</> XML Messages

🕒 Request history

This functionality allows for the check of the fees charged by KDPW with the participation type and the number of reports submitted in selected months.

III.3. XML Messages

The tab enables to send xml reports, filter, view and download sent reports. The filters allow to choose the reports sent "IN" and "OUT" of KDPW, and to select reports depending on the message type and date & time. Types of supported messages:

- auth.rpt.001.01 – used to send reports to ARM with the same structure as auth.016.001.01 plus additional fields for SHORTCODE replacing full personal data;
- auth.str.001.01 – auth.rpt.001.01 status message;
- auth.016.001.01 – notification sent to ARM participants with a copy of the report to the Supervisor (Supervisor report is sent if successfully processed);
- auth.clt.001.01 – used to report data of individuals or entities identified with a SHORTCODE in reports;
- auth.stc.001.01 – auth.clt.001.01 status message;
- auth.enr.001.01 – supplementary message used to report additional transaction details not available from GPW/BondSpot systems;
- auth.ste.001.01 – auth.enr.001.01 status message;
- admi.err.001.01 – feedback message for each input message non-compliant with the XSD of ARM messages and each message unknown to ARM.

After finding the needed data, it is possible to show contents or download in xml format. To do this, click on the + sign to see the details.

XML Messages					Refresh	Upload XML message
Direction	Sender	Receiver	Message type	Date and time		
<input type="text"/>			<input type="text"/>	yyyy-MM-dd		
+ OUT	0001	RT19	auth.016.001.01	2021-06-23 11:31:10	...	
+ OUT	0001	RT19	admi.err.001.01	2021-06-23 11:14:46	...	
+ IN	RT19	0001	auth.rpt.001.01	2021-06-23 11:14:44	...	
+ OUT	0001	RT19	auth.str.001.01	2021-06-23 11:12:08	...	
+ IN	RT19	0001	auth.rpt.001.01	2021-06-23 11:11:01	...	
+ OUT	0001	RT19	auth.str.001.01	2021-06-23 11:09:31	...	

In the upper right corner, there is the "Upload XML message" button, through which the ARM participant can send several types of messages from the station located on the Participant's side, where the xml report was prepared. The following messages may be forwarded to the ARM using button "Upload XML message" functionality.

After selecting the appropriate xml file, the participant approves the choice by clicking "Upload". After the file has been successfully sent, the confirmation is displayed on the screen. The submitted xml report is visible then in the "XML Messages" and "Request history" tabs.

The processing of transmitted messages (reports) is carried out in accordance with the KDPW ARM functional documentation.

After receiving the message, the ARM system performs an on-line validation and returns its results through the appropriate feedback message. The status message is then visible in the "XML Messages" tab. Accepting the message does not mean accepting the reports it contains, and for this purpose the status message should be checked.

III.4. Request history

The tab presents historical reports sent by a participant with information about their acceptance or rejection. It is possible to filter between submitted reports (using the form) and xml files loaded into the GUI. You can also view both reporting methods.

+ RT19	New report	2021-11-17 15:23:27	Waiting: Sent
+ RT19	New report	2021-10-25 20:51:50	Waiting: Sent
+ RT19	New report	2021-10-25 20:43:07	Waiting: Sent
+ RT19	Uploaded XML message	2021-10-22 13:26:34	✓ Accepted
+ RT19	Uploaded XML message	2021-10-22 13:21:56	✓ Accepted