

SCP/ZW/2/2023

Warsaw, 8 May 2023

EMIR TR Participants
SFTR TR Participants
ARM Participants**Re.: Amendments to KDPW regulations in connection with the implementation of IT system changes in A2A communication**

Dear Madam or Sir,

Further to the information provided in our letter of 20 March 2023 (SCP/ZW/1/2023) regarding changes to A2A communication in the KDPW Group services, please be advised that the following will come into effect on 22 May 2023:

- 1/ the new Rules of Establishing Electronic Communication via System Connections, adopted by Resolution No. 356/2023 of the KDPW Management Board of 27 April 2023,
- 2/ amendments to the Rules of Access to the KDPW IT Systems, adopted by Resolution No. 357/2023 of the KDPW Management Board of 27 April 2023,
- 3/ amendments to the ARM Rules, adopted by Resolution No. 358/2023 of the KDPW Management Board of 27 April 2023,
- 4/ amendments to the Terms and Conditions of Communication with the Derivatives Repository, adopted by Resolution No. 359/2023 of the KDPW Management Board of 27 April 2023,
- 5/ amendments to the Terms and Conditions of Communication with the Securities Financing Transactions Repository, adopted by Resolution No. 360/2023 of the KDPW Management Board of 27 April 2023,
- 6/ amendments to the Rules of Registration and Maintenance of Legal Entity Identifiers by KDPW, adopted by Resolution No. 361/2023 of the KDPW Management Board of 27 April 2023.

Documents are introducing new rules for communication using the A2A interface in the following services: EMIR Transaction Repository, SFTR Transaction Repository, ARM, and LEI issuance.

The amendments are available on KDPW's website under the tab Participants/Rules: <https://www.kdpw.pl/en/rules.html>.

Attached hereto* is a detailed description of the procedure for obtaining the new A2A electronic certificates and the parameters for connection to the KDPW systems using MQ queues (Appendices 1-3). Certificates under the new rules will be downloaded via the A2A Certificates application available on the Service Portal (<https://online.kdpw.pl>). After getting access the application, a person authorised by the participant can download certificates for production communication and for testing. The application will not be available in any of the Services Portal test environments.

Please be advised that existing electronic certificates which do not expire before the effective date of the changes can only be used for communication with KDPW until 30 November 2023, unless they expire earlier. After this date, communication using these certificates will not be possible and the certificates will be revoked.

In view of the above, to maintain the continuity of A2A communication, it will be necessary to switch your systems to the new rules for establishing communication before the expiry date of the active certificates but no later than 30 November 2023. We therefore request that you individually arrange with KDPW a date convenient for you for the switchover within the switchover windows scheduled by KDPW (see Appendix 3 for details*). Please send the relevant declaration by the end of June 2023 to the dedicated e-mail address: a2a@kdpw.pl. If you would like to make the switchover in June, please send your declaration by the end of May.

Please note that in connection with the new model for establishing A2A communication, we are making a functional separation between the IT area for downloading certificates and establishing secure system connections and the business area, i.e., reporting. This is particularly important for you to ensure that the person who will be downloading the new electronic certificate has the necessary IT qualifications (see Appendix 3 for details).

Yours sincerely,
Sławomir Panasiuk
Vice President

Attachments*:

- 1/ Specification of MQ configuration in A2A communication
- 2/ Instructions for downloading A2A certificates
- 3/ Description of the implementation of changes in A2A communication
- 4/ Using OpenSSL to obtain a certificate for A2A communication

* the attachments contain information protected by KDPW and have been made available directly to the addressees of the letter