Krajowy Depozyt Papierów Wartościowych S.A.
KDPW_CCP S.A.
ul. Książęca 4
00-498 Warszawa

T 22 537 93 43 | 22 537 91 27
F 22 627 31 11
E kdpw@kdpw.pl | ccp@kdpw.pl
www.kdpw.pl | www.kdpwccp.pl

SCP/ZW/1/2023
CCP/ZW/242/2023

Warsaw, 20 March 2023

To: KDPW Participants
KDPW_CCP Participants
EMIR TR Participants
SFTR TR Participants
ARM Participants

Re.: Changes to IT systems in the area of A2A communication

Dear Madam or Sir,

Further to the information provided in our letter of 4 October 2022 (our ref.: SCP/ZW/8/2022 and CCP/ZW/655/2022) outlining the KDPW Group's planned changes to its IT systems, we present information describing the scope of the planned changes in the area of the use of electronic certificates in A2A communication.

The work undertaken by the KDPW Group in this area is aimed at continuously improving the security of the IT systems used in the services provided to you in response to new risks to cyber security. In this regard, secure connections between IT systems in the A2A model are particularly relevant, both for the communication and in the context of ensuring the continuity of services. At the same time, we are standardising A2A communication functions across all services provided by the KDPW Group.

As part of the planned changes, we will modernise the issuing and use of electronic certificates used for authentication in MQ-based communication systems. Furthermore, the certificates will no longer be personal, their construction will be standardised (in particular by introducing uniform cryptographic algorithms), as will their secured storage, and the use of certificates will be uniform across all KDPW Group services. The process of applying for a certificate will be handled by a dedicated application within the Services Portal online.kdpw.pl based on a private key generated directly by the applicant. Moreover, uniform rules will be introduced as regards segregation of services within A2A communication, unification of names in queue configuration, and management of access to test environments.

Krajowy Depozyt Papierów Wartościowych Spółka Akcyjna z siedzibą w Warszawie (00 -498) przy ulicy Książęcej 4, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr KRS 0000081582, NIP 526 -10-09-528, wysokość kapitału zakładowego i kapitału wpłaconego - 21.000.000 zł.

KDPW_CCP Spółka Akcyjna z siedzibą w Warszawie (00 -498) przy ul. Książęcej 4, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr KRS 0000357452, NIP: 701- 02-37-032, wysokość kapitału zakładowego i kapitału wpłaconego - 190.000.000 zł.

We provide a detailed description of the changes in the annex to this letter.

The changes will be implemented in two steps.

In the first step, the changes will cover the A2A communication of the EMIR TR, SFTR TR, ARM (excluding SWI communications), and LEI services – implementation of these changes is scheduled for **April/May 2023**.

The second step will include modernisation of SWI communication, i.e., services for KDPW direct members (including ARM and Compensation Scheme services) and KDPW_CCP clearing members. This implementation is planned for **April 2024**.
Details of the detailed implementation timeline together with the new connection parameters for the individual services will be communicated to you separately in each step of the process.

Yours sincerely,

Annex:
Specification of the planned changes for the modernisation of A2A communication

C/C:
Chamber of Brokerage Houses (IDM)
Council of Depositary Banks at the Polish Bank Association (RBD ZBP)
Polish Financial Supervision Authority (UKNF)

Annex: Specification of the planned changes for the modernisation of A2A communication

The modernisation of communication channels for the exchange of messages in the A2A model and changes to the issuing and maintenance of electronic certificates will include the following changes.

Issuing certificates

- Electronic certificates will be used, as is currently the case, to establish a secure encrypted system connection between the participant and the KDPW Group's IT systems. A certificate will be issued to a participant's institution code, which is the participant's four-character identifier in the relevant KDPW Group service(s) according to the established scheme.
- Electronic certificates, and in particular applications for their issuance, the downloading of certificates and the revocation of certificates, will be handled by a dedicated certificate management application ("A2A Certificates") available to participants within the Service Portal (https://online.kdpw.pl). Only the person authorised by the participant to carry out certificate management activities on the participant's behalf will have access to the application. Authentication and authorisation in the application will take place according to uniform rules applicable to all Service Portal applications.
- Each person authorised by the participant under the institution code will be authorised to request the generation of a certificate(s) (it is expected that there will be a limit on the number of certificates that can be issued) active for the certificate code. It will be possible to re-download a generated certificate and to revoke a selected certificate.
- Certificates will be generated and issued on the basis of PKI mechanisms, using the SHA-256 algorithm, following a request submitted by the entity, signed with the private key. The private key will be generated directly by the entity requesting a certificate within its own infrastructure, e.g., based on OpenSSL mechanisms. In its dedicated certificate management service for A2A communication, KDPW will provide a description of the process that will allow all steps to be performed by the participant's in-house IT services. NOTE: The private key must not be made available to unauthorised persons, and it must not be transferred to KDPW.
- Issuing a certificate and making it available for download will each time require KDPW's approval of the submitted request, including a check of the request.

Establishing A2A connections

- Issued and downloaded certificates for A2A communication will be used to communicate with all services where A2A communication is foreseen and where the entity is acting under the institution code assigned to the certificate. The certificate will enable the establishment of encrypted TLS communication and authentication within the MQ communication channels dedicated to the institution code.
- At A2A communication level, communication will be separated by service supported by the KDPW Group's dedicated IT solutions. This means that dedicated MQ queues will be created for each service (separately for each direction of information exchange).

- The separation of communication under an institution code will involve separate queues for A2A communication for the following services where A2A communication is available (queues will be configured only for entities actually acting and using A2A communication in the service):
    - CSD – core services of the depository and clearing system (alignment in step 2 of implementation)
    - CCP – clearing services provided by KDPW_CCP (alignment in step 2 of implementation)
    - EMIR – EMIR Trade Repository reporting services (step 1)
    - ARM – ARM reporting services (step 1, alignment of communication in SWI is expected in step 2 of implementation)
    - SFTR – SFTR Trade Repository reporting services (step 1)
    - LEI – LEI issuance automation services (step 1)
    - SR – Compensation Scheme services for direct participants (alignment in step 2 of implementation)
- Depending on the way the service operates and the associated expected performance parameters, dedicated A2A communication queues can be created within one or more dedicated communication channels. Detailed connection parameters, including IP addressing and names of individual components, will be presented within the certificate management application available through the Service Portal only to persons who are granted access to the application under an authorisation granted to them by the participant.
- No changes are expected in the current communication protocols, which ensures that the message structures need not be adapted.

Handling the test environments

- In the handling of the test environments, the naming model will be standardised by introducing names in line with those used in the Service Portal (U2A channel). The educational environment will be labelled EDU and the test environment for new functionalities will be labelled TST. The current names TSTA and TSTB will be no longer in use.
- We will maintain the principle of using a single certificate for access to the EDU and TST environments while communication will be separated using separate queues for each environment (also by service).
- Requests for certificates to use the KDPW Group's application test environments will be handled according to the same principles as requests for certificates for communication in the production environment, in the dedicated certificate management application in the Services Portal ("A2A Certificates").

Technical connection parameters

- The following minimum requirements are expected as the security standards for telecommunications connections using VPN/IPSec technology:
    - IKE Version – V2
    - Integrity (Hashing Algorithm) – SHA-256

○ Encryption Algorithm	– AES-256
○ Key exchange	– Diffie-Hellman Group 19

Regulatory model

- Under the regulatory model for A2A communications, there will be separate rules for establishing system connections. The current Rules of Access to the KDPW IT System will govern only the rules of access to KDPW's U2A application interfaces, and the second step of implementation of the system changes will involve the relevant amendment of the SWI Agreements and the SWI Rules. This regulatory model will allow us to centralise the description of access rules and dedicate individual areas to entities that use particular forms of communication in practice.
- The implementation of the changes will amend the rules of individual services using A2A communication.