THE RULES FOR ESTABLISHING ELECTRONIC COMMUNICATION THROUGH SYSTEM CONNECTIONS

Chapter 1

General

§ 1

1. The Rules for establishing electronic communication through system connections, hereinafter „the Rules", define the principles for issuing electronic certificates, authenticating communication channels and establishing communication with applications using the A2A interface.
2. These Rules shall be applied to legal relations arising from agreements concluded by KDPW with participants or other entities that receive services provided by KDPW or KDPW_CCP, which are available via KDPW's IT systems.
3. The provisions of these Rules shall be applied accordingly to legal relations arising from agreements concluded with entities that have only been granted access to the test environment of IT systems, referred to in subpara. 2.

§ 2

Whenever the following terms are used herein:

1) application – this shall be understood to mean any application used for electronic communication with KDPW or KDPW_CCP as part of a specific service, enabling the exchange of messages using data transmission, available via an A2A interface, operating within the KDPW infrastructure;
2) A2A interface – this shall be understood to mean an interface supporting automated exchange of data between the application and a participant's application using dedicated message queues;
3) electronic certificate – this shall be understood to mean a certificate issued by KDPW, used to establish encrypted electronic communication using an A2A interface between the participant's system and the application (applications);
4) service – this shall be understood to mean a service provided by KDPW or KDPW_CCP, made available to participants via an application;
5) participant – this shall be understood to mean an entity, which is a party to a participation agreement concluded with KDPW on the basis of the relevant service rules, or another entity, including a KDPW_CCP participant, that receives access to an application via an A2A interface on the basis of a agreement concluded with that entity;
6) service rules – this shall be understood to mean a template agreement which defines the legal relationship, applicable to a specific service, or another agreement, on the basis of which electronic communication is made available to the participant;
7) Access Rules – this shall be understood to mean the Rules of Access to the KDPW IT Systems, approved by a separate Resolution of the KDPW Management Board;
8) message – this shall be understood to mean information or a declaration which, under the service rules, may or should be transmitted via means of electronic communication;

9) electronic communication – this shall be understood to mean the submission and receipt of declarations of intent and information which, under the service rules, in relations between KDPW and KDPW_CCP, may or should be transmitted by or to the participant via an application KDPW;
10) certificate management – this shall be understood to mean actions performed by the participant related to the submission or receipt of statements in relation to the generation of an electronic certificate, its download and its cancellation;
11) institution code – this shall be understood to mean a four-character code assigned by KDPW to a participant, which is the participant's identifier within a given service or many services
12) KDPW – this shall be understood to mean the company known as Krajowy Depozyt Papierów Wartościowych S.A.;
13) KDPW_CCP – this shall be understood to mean the KDPW subsidiary, KDPW_CCP S.A.

§ 3

KDPW is not a qualified trust service provider within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (EU Journal of Laws L 257, p. 73).

Chapter 2

Electronic certificates

§ 4

1. In order to establish electronic communication using the A2A interface, the participant should obtain an electronic certificate.
2. An electronic certificate is issued for a given participant's institution code and may be used to establish communication with all services that the participant receives under this code. KDPW may limit the number of electronic certificates that can be generated and issued for each single institution code.
3. A participant who, in accordance with the terms and conditions of the service, may use or is obliged to use electronic communication via the A2A interface, should gain access to the dedicated A2A Certificates application made available by KDPW as part of the Services Portal https://online.kdpw.pl, for the purpose of certificate management.
4. The rules for obtaining access to the A2A Certificates application by a person authorised by the participant to act on their behalf, the rules for opening an access account by such a person and the rules for carrying out the authentication process shall be defined in the provisions of the Access Regulations.
5. A participant may authorise more than one person to manage certificates within a given institution code.
6. A person authorised by the participant to manage certificates may only access the A2A Certificates application as a user. Requests for access by this person shall only be accepted or rejected by KDPW.
7. A person who has obtained access to the A2A Certificates application on behalf of a participant may, using this application, manage certificates, which are used for communication with the production or test environments of applications in which this participant performs actions under a given institution code, subject to the provisions of subpara. 8.
8. A person authorised by an entity that has not yet concluded a participation agreement within a specific service, may, until the date of the conclusion of such an agreement, only use the A2A

Certificates application to manage certificates necessary for communication with the application test environment.

9. A person who has gained access to the A2A Certificates application on behalf of the entity referred to in § 1 subpara. 3, may only manage certificates necessary for communication with the application test environment. The agreement on granting such an entity access to the test environment of the application shall be deemed to be concluded from the moment when KDPW grants that person access to the A2A Certificates application.

§ 5

1. Electronic certificates shall remain valid for the period indicated in the contents of the certificate itself, and subject to the certificate's validity period set by the issuing certification authority for that electronic certificate.

2. Participants shall regularly monitor the validity of obtained electronic certificates.

3. KDPW may, before the expiry of the term referred to in subpara. 1, revoke an electronic certificate at its own initiative for technical reasons, or due to suspected unapproved use of the electronic certificate by a person not authorised by a participant.

4. KDPW shall make a certificate revocation list (CRL) available to participants on its website, in order to verify the validity of certificates. Immediately following the revocation of a certificate, information on the revocation of that electronic certificate shall be added to the list.

5. If an electronic certificate is revoked, KDPW shall immediately send the participant notification of this fact to the e-mail addresses being the login of persons authorised by the participant who have access to the A2A Certificates application.

§ 6

1. A participant shall be obliged to store the electronic certificate in a way that ensures that only authorised persons have access to the certificate. From the moment that the certificate has been issued until its revocation, liability for its loss or disclosure rests solely with the participant.

2. In the event of the loss of an electronic certificate, or whenever there are justifiable grounds to suspect that an electronic certificate has been made available to an unauthorised person, the participant who has obtained the electronic certificate shall be obliged to immediately revoke this certificate via the A2A Certificates application.

3. KDPW shall not be liable for any damage caused to a participant in connection with the loss of an electronic certificate during its validity period.

Chapter 3

Electronic communication using the A2A interface

§ 7

1. Electronic communication using the A2A interface is only possible if permitted by the communication rules within a given service.

2. An electronic certificate may be used for electronic communication within the scope of all services

to which the participant has access or will have access in future under a given institution code.

3. Electronic communication via the A2A interface relies on message queues used to transmit messages.

4. Initiating electronic communication via the A2A interface requires:
   1) authentication by the participant to use a communication channel dedicated to a given application, using the electronic certificate they have been issued with, and
   2) KDPW to assign to the participant message queues to be used within a given service.

5. Message queues are created within the communication channel that is used within a given service. Message queues are assigned to a participant by KDPW after having obtained participation status within a given service.

6. Communication channels may be established independently for each application. A single communication channel may also be used to access more than one application by means of dedicated queues.

7. Queues are created separately for each service for which A2A communication is available. Within already established communication, pairs of queues may be set up separately for each direction of communication. Service rules may also provide for the creation of an additional output or input message queue for the transmission of dedicated information.

8. Communication within a communication channel is secured with TLS encryption.

9. Connectivity with the KDPW infrastructure is available in both the client-to-server and the server-to-server model. A VPN connection is required with pre-shared key authentication.

10. KDPW shall reserve the right to delete messages not received by the participant from message queues 30 days after the message is sent by KDPW, or within a shorter time limit if so agreed with the participant and, in the case of test environments, after 7 days from the date of transmission of the message. Service rules may also provide that messages transmitted by KDPW have a specific validity period, after which, if not received by the participant, they shall be automatically removed from the output queues.

11. KDPW's obligation to deliver the message referred to in sub-para. 10 to a participant shall expire at the end of the period specified in accordance with that provision.

§ 8

1. Subject to the provisions of subpara. 2-4, electronic communication shall be available to participants on a 24/7 basis.
2. KDPW may introduce a technical break in the operation of an application, in accordance with the principles described in the service rules or the communication rules adopted for a given service.
3. Communication via the A2A interface may be subject to interruptions of the availability of message queues due to technical breaks lasting several minutes, related to the reconfiguration of the settings of such queues.
4. When using the A2A interface to communicate with applications, participants shall be obliged to configure their systems to permit the automatic resumption of the connection to the communication queues.

§ 9

1. Messages sent by the participant via the A2A interface shall be deemed delivered upon the receipt of the message by KDPW, where the receipt of the message shall be defined from the commencement of the validation of this message in the KDPW application. Messages sent to a participant via the A2A interface shall be deemed delivered from the moment of their entry in the participant's output queue.

2. The rules governing communication for each specific service may impose additional obligations on participants in connection with the transmission of messages, in particular authentication or confirmation of identity of the person transmitting the message or signing messages with an electronic signature.

3. Participants shall acknowledge the legal effectiveness of the delivery of messages, subject to the conditions provided for in these Rules, and shall consent to any measures to obtain evidence that such actions have been performed.

4. The Participant shall consider the declarations and the information sent using the A2A interface as being its own.

Chapter 4

Final provisions

§ 10

1. KDPW shall have the right to amend these Rules.

2. KDPW shall make any amendment to these rules available to participants on its website. Amendments shall come into force within two weeks from the date on which they are made available, unless a resolution of the KDPW Management Board implementing the amendments indicates a later date.

3. Any amendments of these Rules and the date of their coming into force shall be notified to participants within the time limit referred to in subpara. 2.

4. The transmission of information concerning an amendment to the Rules by email sent to the email address that is the log-in of a person authorised by a participant to access the A2A Certificates application shall be deemed legally effective notification of the amendment to the participant, unless the service rules provide otherwise.

5. If a participant refuses to accept an amendment to the Rules, the participant shall have the right to terminate the service agreement, subject to the terms and conditions of termination under the service rules.

6. Unless a participant terminates the participation agreement according to subpara. 5, the participant shall be deemed to have accepted the amendment to the Rules of which they were notified.