Appendix 3: Instructions for downloading the A2A certificates used for connecting to the KDPW and KDPW_CCP services

This appendix describes the A2A certificate scheme in communication with the KDPW and KDPW_CCP services and how to generate and download a certificate using dedicated applications (separately for KDPW and KDPW_CCP) available on the Services Portal (https://online.kdpw.pl).
After gaining access to this application, a person authorized by the participant can download both certificates for production communication and tests. At the same time, the application will not be available in any of the Service Portal test environments.

Electronic certificates used for A2A communication

- To establish secure communication with KDPW Group services based on MQ queues in the A2A model, KDPW and KDPW_CCP use electronic certificates based on asymmetric cryptography within the Public Key Infrastructure (PKI).
- An electronic certificate is issued for a participant’s institution code and can be used to establish communication for access to all services where the participant appears under that code (separately for KDPW and KDPW_CCP). The certificate is used to establish an encrypted connection based on the TLS protocol and to authenticate the user in the relevant communication channel within A2A communications based on MQ queues.
- In A2A communication, KDPW has established the following certificate scheme:
    - Key type: - RSA
    - Key size: - 2048
    - Entity name X.509:
        - Organization Name (O=[A-Z0-9]{4,4}) - institution code, e.g. XXXX
        - Organizational Unit Name (OU=[PRD;TST]) - environment name
        - Common Name (CN= [A-Z0-9]{4,4}+“_A2A”) - common name, e.g. XXXX_A2A
- In A2A communication, KDPW_CCP has established the following certificate scheme:
    - Key type: - RSA
    - Key size: - 2048
    - Entity name X.509:
        - Organization Name (O=[A-Z0-9]{4,4}) - institution code, e.g. XXXX
        - Organizational Unit Name (OU=[PRD;TST]) - environment name
        - Common Name (CN= [A-Z0-9]{4,4}+“_CCPA2A”) - common name, e.g. XXXX_CCPA2A
- Only certificates generated in accordance with the scheme established for A2A communications and signed by KDPW may be used to establish communications.

Description of the A2A certificate generation process

- A certificate is generated and issued using PKI mechanisms and the SHA-256 algorithm. The process of obtaining a certificate is carried out in several steps, with the security of the private key ensured. Throughout the process, the private key of the participant requesting the certificate is not disclosed to KDPW (it should be secured within the infrastructure of the certificate owner).

- A certificate is obtained based on a Certificate Signing Request (CSR) transmitted by the applicant, generated and saved in PEM format.
- A Certificate Signing Request is generated directly by the applicant within its own infrastructure, e.g. using OpenSSL mechanisms. This requires appropriate IT expertise and access to tools for generating private keys and CSRs.
- When creating a Certificate Signing Request, the applicant must ensure that it complies with the established scheme to the extent of the key type and length and the data comprising the Distinguished Name (DN), in particular the institution code and the environment code.
- The management of electronic certificates to the extent of requesting a certificate, downloading a certificate and revoking a certificate, is possible through a dedicated certificate management application available within the Services Portal (https://online.kdpw.pl). Only a person authorised by the participant for certificate management on its behalf can access the application.
- A Certificate Signing Request is transmitted in the form of a request in the dedicated application, to which it is attached in text form. In the preparation of the request, the application verifies the conformity of the information contained in the CSR with the certificate scheme, including the institution code in the context of which it is submitted.
- A Certificate Signing Request must be created in PKCS#10 format using PEM encoding.
- Once the CSR has been processed, the application will enable the download of a certificate generated and signed by KDPW, which can be used within the participant's infrastructure to establish a TLS connection and authenticate in the MQ communication channel within the A2A communication. The applicant may, within its own infrastructure, combine the received certificate with a previously generated private key in the form of a PKCS#12 container.

NOTE: Continuous access to A2A channel services requires a valid certificate. Participants should monitor the validity of certificates and request the generation of a new certificate in due time. Participants may also request more than one certificate for a given institution code.

Participants should keep electronic certificates and private keys in a secure location. In the event of loss of the private key or in the event of any security breach, participants must revoke the certificate using the dedicated application. Once revoked, the certificate will be placed on the Certificate Revocation List (CRL), which is published at: http://pki.kdpw.pl/crl/kdpw-cck1.crl.