KDPW

<u>Załącznik 1</u>: Specyfikacja konfiguracji MQ w komunikacji A2A

Niniejszy załącznik opisuje parametry wymagane do zestawienia połączenia MQ w ramach komunikacji A2A, ze wskazaniem zmian względem dotychczasowej konfiguracji. Opracowanie stanowi całościowy opis wraz z modyfikacjami wprowadzonymi w ramach II etapu projektu. Elementy wymagające zmiany związane z obecnie wprowadzanymi zmianami względem dotychczasowych parametrów zostały wyróżnione wytłuszczonym drukiem i podkreśleniem.

Ustanowienie połączenia A2A

- Wygenerowany i pobrany certyfikat A2A będzie wykorzystywany do komunikacji ze wszystkimi usługami, w ramach których przewidziana jest komunikacja A2A i w ramach których, dany podmiot występuje pod tym samym kodem instytucji. Certyfikat służy do ustanowienia szyfrowanej komunikacji TLS oraz uwierzytelnienia w ramach dedykowanych dla danego kodu instytucji kanałów komunikacyjnych MQ.
- Na poziomie komunikacji A2A zapewniona zostanie separacja komunikacji w podziale na poszczególne usługi obsługiwane przez dedykowane rozwiązania informatyczne GK KDPW. Oznacza to, że dla każdej usługi tworzone będą dedykowane kolejki MQ (odrębnie dla każdego z kierunków wymiany informacji).
- Wprowadzenie separacji komunikacji w ramach danego kodu instytucji obejmować będzie odrębne kolejki do komunikacji A2A dla następujących usług (kolejki zostaną skonfigurowane jedynie dla podmiotów faktycznie występujących i korzystających z komunikacji A2A w danej usłudze):
    - EMIR – usługa raportowania do Repozytorium Transakcji EMIR (do czasu wprowadzenia zmian REFIT)
    - ETR – usługa raportowania do Repozytorium Transakcji EMIR (po zmianach REFIT)
    - ARM – usługa raportowania do ARM
    - SFTR – usługa raportowania do Repozytorium Transakcji SFTR
    - LEI – usługa automatyzacji nadawania kodów LEI
    - CSD – usługi udostępniane w ramach systemu depozytowo-rozrachunkowego
    - ICS – usługa obsługi Systemu Rekompensat
- Wprowadzenie separacji komunikacji w ramach usług Spółek GK KDPW, w szczególności wyodrębnienie usług KDPW_CCP na bazie odrębnego certyfikatu elektronicznego oraz parametrów połączeniowych, w tym także odrębnych kolejek do komunikacji A2A dla następujących usług:
    - CCP – usługi rozliczeniowe KDPW_CCP

Parametry dla połączeń telekomunikacyjnych

- W obszarze standardów zabezpieczeń dla połączeń telekomunikacyjnych wykorzystujących technologię VPN/IPSec przewiduje się następujące minimalne wymagania:
    - Protokół – **<u>IKEv2/IPSec (ESP)</u>**
    - Funkcja skrótu – SHA-256
    - Algorytm szyfrowania – AES-256

  - Protokół wymiany kluczy – Diffie-Hellman Group 19
- Parametry łączy w ramach sieci MPLS (bez zmian):
  - Typ sieci – L3
  - Routing – BGPv4

Parametry połączenia oraz komunikacji MQ w ramach komunikacji ESDK

- Nazwa managera kolejek MQ dla komunikacji A2A z usługami KDPW:
  - Nazwa dla środowisk PRD i BCM – **A2AEPRD**
  - Nazwa dla środowisk EDU i TST – **A2AETST**
- Nazwa managera kolejek MQ dla komunikacji A2A z usługami KDPW_CCP:
  - Nazwa dla środowisk PRD i BCM – **CCPA2AEPRD**
  - Nazwa dla środowisk EDU i TST – **CCPA2AETST**
- Adresacja TCP/IP **ulegnie zmianie** – adresacja IP oraz numery portów zostaną wskazane na dalszym etapie
- Atrybuty konfiguracyjne managerów MQ zmienione względem nastaw domyślnych lub szczególnie istotne:
  - CCSID – 819
  - MAXMSGL – 104 857 600
  - VERSION – **09030015**
- Nazewnictwo kanałów MQ dla poszczególnych środowisk - ***prefix.senv.code.con***:
  - prefix – stały element nazwy kanału:
    - A2AE – środowiska KDPW oparte o komunikację ESDK
    - CCPA2AE – środowiska KDPW_CCP oparte o komunikację ESDK
  - senv – kod środowiska (PRD, EDU, TST, BCM)
  - code – kod instytucji Uczestnika w ramach kanału
  - con – typ połączenia:
    - C – server-connection (*SVRCN) dla klient-serwer
    - KP – KDPW->Uczestnik dla serwer-serwer, receiver (*RCVR) po stronie Uczestnika
    - PK – Uczestnik->KDPW dla serwer-serwer, sender (*SDR) po stronie Uczestnika
- Atrybuty konfiguracyjne kanałów MQ zmienione względem nastaw domyślnych:
  - COMPMSG – ZLIBFAST
  - DISCINT – 6000
  - MAXMSGL – 104 857 600
  - SSLCIPH – **TLS_AES_256_GCM_SHA384**
  - SSLPEER – Common Name (CN) certyfikatu drugiej strony połączenia:
    - Środowisko PRD – CN=**A2AEPRD** (dla KDPW_CCP CN=**CCPA2AEPRD)**
    - Środowisko EDU – CN=**A2AETST** (dla KDPW_CCP CN=**CCPA2AETST)**
    - Środowisko TST – CN=**A2AETST** (dla KDPW_CCP CN=**CCPA2AETST)**
    - Środowisko BCM – CN=**A2AEPRD** (dla KDPW_CCP CN=**CCPA2AEPRD)**
- Atrybuty konfiguracyjne kolejek MQ zmienione względem nastaw domyślnych (bez zmian):
  - DEFPSIST – YES
  - MAXMSGL – 104 857 600

- Nazewnictwo kolejek MQ dla poszczególnych środowisk - ***srv.senv.code.direction***
  - srv – oznaczenie usługi (EMIR, ETR, ARM, SFTR, LEI, ICS, CSD, CCP)
  - senv – kod środowiska (PRD, EDU, TST, BCM)
  - code – kod instytucji Uczestnika w ramach kanału
  - direction – typ połączenia:
    - KP – komunikaty od KDPW do Uczestnika
    - PK – komunikaty od Uczestnika do KDPW
- Nazewnictwo kolejek dedykowanych dodatkowym usługom – ***srv.senv.code.direction.postfix***
  - srv – oznaczenie usługi
  - senv – kod środowiska
  - code – kod instytucji
  - direction – typ połączenia (KP, PK)
  - postfix – oznaczenie funkcji zgodnie z regulacjami usługi
- Parametry kodowania komunikatów dla aplikacji klienckich (bez zmian):
  - CodedCharSetId = 1208