

SCP/ZW/1/2024
CCP/ZW/132/2024

Warszawa, 7 lutego 2024 r.

Uczestnicy KDPW
Uczestnicy KDPW_CCP**dot.: zmian w systemach informatycznych w obszarze komunikacji A2A**

Szanowni Państwo,

W nawiązaniu do informacji przekazanych w pismach z dnia 3 października 2023 roku (nasz znak: SCP/ZW/3/2023 oraz CCP/ZW/675/2023) oraz z dnia 20 marca 2023 roku (nasz znak: SCP/ZW/1/2023 oraz CCP/ZW/242/2023), informujących o planowanych przez GK KDPW zmianach w systemach informatycznych, przekazujemy informacje opisujące zakres planowanych zmian w obszarze wykorzystania certyfikatów elektronicznych w ramach komunikacji A2A.

Pierwszy etap projektu, wdrożony w 2023 r., objął zmianami obszary komunikacji A2A w zakresie usług Repozytorium transakcji EMIR, Repozytorium transakcji SFTR oraz ARM (z wyjątkiem komunikacji realizowanej w ramach SWI). W ramach wprowadzonych zmian, opracowana została aplikacja, pozwalająca na zarządzanie certyfikatami elektronicznymi wykorzystywanymi do uwierzytelnienia się systemów do komunikacji opartej o kolejki MQ, przy jednoczesnej zmianie algorytmów szyfrujących oraz ujednoczeniu schematu wykorzystywanego do ich generacji. Wprowadzono również jednolite zasady związane z segregacją usług w ramach komunikacji A2A, ujednoczeniem nazewnictwa w obszarach konfiguracji kolejek oraz zarządzaniem dostępem do środowisk testowych.

W ramach przyjętego modelu, certyfikat elektroniczny służy do ustanowienia bezpiecznego szyfrowanego połączenia systemowego pomiędzy uczestnikiem a systemami informatycznymi GK KDPW. Certyfikat wystawiany jest na dany kod instytucji uczestnika, będący czteroznakowym identyfikatorem uczestnika w danej usłudze lub usługach, zgodnie z ustalonym schematem. Obsługa certyfikatów, a w szczególności złożenie wniosku o jego wystawienie, pobranie certyfikatu oraz unieważnienie certyfikatu, jest możliwa poprzez aplikację Certyfikaty A2A, dostępną w ramach Portalu

usług (<https://online.kdpw.pl>), która wraz z wdrożeniem drugiego etapu projektu będzie udostępniona również uczestnikom bezpośrednim KDPW. Analogiczna aplikacja zostanie udostępniona uczestnikom rozliczającym KDPW_CCP. Dostęp do aplikacji Certyfikaty A2A może uzyskać wyłącznie osoba upoważniona przez uczestnika do podejmowania w jego imieniu czynności związanych z obsługą certyfikatów. Zarówno proces uwierzytelniania jak i uzyskania autoryzacji do aplikacji odbywa się na zasadach obowiązujących dla wszystkich aplikacji w ramach Portalu usług. Każda osoba upoważniona przez uczestnika jest uprawniona do wnioskowania o wygenerowanie aktywnych na dany kod certyfikatów. Jednocześnie możliwe jest powtórne pobranie już wygenerowanego certyfikatu oraz unieważnienie wskazanego.

Obecnie realizowane prace, stanowiące drugi etap projektu modernizacji i standaryzacji komunikacji A2A, obejmują implementację zmian w zakresie komunikacji SWI (realizowanej zgodnie z obecnie obowiązującym Regulaminem SWI), czyli w obszarze dotyczącym usług dla uczestników bezpośrednich KDPW (w tym także w ramach usług ARM oraz Systemu Rekompensat) oraz uczestników rozliczających KDPW_CCP. W praktyce oznacza to wprowadzenie odrębnych kolejek MQ dla poszczególnych usług: systemu depozytowo-rozrachunkowego, Systemu Rekompensat, ARM (z wykorzystaniem protokołu ESDK), a także usług rozliczeniowych świadczonych przez KDPW_CCP. Komunikacja SWI realizowana w ramach usługi ARM bez wykorzystania protokołu ESDK będzie przełączona do dedykowanego dla tego rodzaju połączenia punktu dostępowego, uruchomionego w trakcie I etapu projektu.

Na poziomie GK KDPW wprowadzona zostanie separacja w zakresie uwierzytelniania się do komunikacji MQ. Oznaczać to będzie konieczność wystąpienia o odrębne certyfikaty celem ustanowienia komunikacji A2A z KDPW oraz z KDPW_CCP.

Poza zmianą parametrów połączeniowych oraz modyfikacją sposobu wydawania certyfikatów elektronicznych, w ramach wprowadzanych zmian, przewiduje się również odejście od wymogu podpisywania komunikatów ESDK wydanym certyfikatem. W tym zakresie modyfikacji ulegnie ramka protokołu ESDK, a proces zapewnienia integralności przesyłki oparty zostanie o wbudowane mechanizmy obsługi kolejek MQ.

Szczegółowy opis wprowadzanych zmian, a także dokumentację poszczególnych rozwiązań, przekazujemy w załączniku do niniejszego pisma.

Wdrożenie całości rozwiązania przewidziane jest na **grudzień 2024 roku**. Wdrożenie wiązać się będzie z umożliwieniem uczestnikom bezpośrednim KDPW oraz uczestnikom rozliczającym KDPW_CCP dostępu do aplikacji obsługujących wydawanie certyfikatów, a także z zaprzestaniem wydawania certyfikatów w ramach obecnego centrum autoryzacji. Wszystkie certyfikaty pobrane wcześniej będą mogły być wykorzystywane do czasu przełączenia komunikacji na nowe, zmodernizowane rozwiązanie lub ich unieważnienia.

Przełączenie uczestników na nowy model komunikacji A2A realizowane będzie po wdrożeniu zmian, począwszy od grudnia 2024, w ramach ustalonych okien przełączeniowych (plan okien przełączeniowych zostanie zakomunikowany na końcowym etapie przedsięwzięcia), odrębnie

dla środowisk testowych (TST i EDU) oraz dla środowiska produkcyjnego (PRD). W ramach każdego z okien przełączeniowych, przełączana będzie komunikacja dla grupy kodów instytucji zgodnie z przyjętymi od uczestników deklaracjami. W celu zminimalizowania wpływu procesu przełączania na procesy biznesowe, prace w obszarze środowiska produkcyjnego planowane będą wyłącznie na soboty.

Bazując na doświadczeniach z I etapu przewidujemy, że dla wszystkich kodów instytucji przełączenie powinno zostać wykonane w przeciągu **3-4 miesięcy**. Po zakończeniu procesu, wszystkie certyfikaty wydane w ramach obecnie funkcjonującego centrum autoryzacji zostaną unieważnione.

Wdrożenie opisywanych funkcjonalności, będzie się wiązać z koniecznością wprowadzenia zmian również w sferze formalnej, zarówno w regulacjach KDPW, jak i KDPW _CCP.

Szczegółowe informacje związane z procesem przełączenia komunikacji na nowy model, a także informacje o planowanych zmianach w obszarze regulacji, przekazemy Państwu na dalszym etapie prac projektowych.

Z poważaniem,

Sławomir Panasiuk
Wiceprezes Zarządu

Załączniki:

- 1/ Specyfikacja konfiguracji MQ w komunikacji A2A
- 2/ Opis protokołu ESDK wykorzystywanego w ramach komunikacji A2A
- 3/ Instrukcja pobrania certyfikatu A2A
- 4/ Wykorzystanie OpenSSL do uzyskania certyfikatu do komunikacji A2A

Do wiadomości:

Izba Domów Maklerskich
Rada Banków Depozytariuszy przy ZBP
Urząd Komisji Nadzoru Finansowego