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

Warszawa, 20 marca 2023 r.

Uczestnicy KDPW
Uczestnicy KDPW_CCP
Uczestnicy RT EMIR
Uczestnicy RT SFTR
Uczestnicy ARM

dot.: zmian w systemach informatycznych w obszarze komunikacji A2A

Szanowni Państwo,

w nawiązaniu do informacji przekazanych w piśmie z dnia 4 października 2022 roku (nasz znak: SCP/ZW/8/2022 oraz CCP/ZW/655/2022) o planowanych przez GK KDPW zmianach w systemach informatycznych, przekazujemy opis planowanych zmian w obszarze wykorzystania certyfikatów elektronicznych w ramach komunikacji A2A.
Podejmowane przez GK KDPW prace we wspomnianym obszarze mają na celu stałe podnoszenie poziomu bezpieczeństwa systemów informatycznych wykorzystywanych w ramach świadczonych na Państwa rzecz usług, co jest odpowiedzią na nowe ryzyka w obszarze cyberbezpieczeństwa. W tym aspekcie bezpieczne połączenie pomiędzy systemami informatycznymi w modelu A2A jest szczególnie ważne, zarówno w obszarze samej komunikacji, jak i w kontekście zapewnienia ciągłości działania usług. Jednocześnie, ujednolicony zostanie sposób funkcjonowania komunikacji A2A w ramach wszystkich świadczonych przez GK KDPW usług.
W ramach wprowadzanych zmian, zmodernizowany zostanie obszar wydawania oraz wykorzystania certyfikatów elektronicznych, wykorzystywanych do uwierzytelnienia się systemów do komunikacji opartej o kolejki MQ. Ponadto przewiduje się odejście od imiennego charakteru certyfikatów, ujednolicenie ich budowy (w szczególności wprowadzenie jednolitych algorytmów kryptograficznych) oraz bezpiecznego miejsca ich przechowywania, a także jednolitego sposobu wykorzystania tych certyfikatów we wszystkich usługach GK KDPW. Proces wnioskowania o wydanie certyfikatu będzie realizowany poprzez dedykowaną aplikację w ramach Portalu usług - online.kdpw.pl, w oparciu o klucz prywatny generowany bezpośrednio przez wnioskującego. Dodatkowo, wprowadzone zostaną

jednolite zasady związane z segregacją usług w ramach komunikacji A2A, ujednoliceniem nazewnictwa w obszarach konfiguracji kolejek oraz zarządzaniem dostępem do środowisk testowych.

Szczegółowy opis wprowadzanych zmian przekazujemy w załączniku do niniejszego pisma.

Zmiany wprowadzane będą w dwóch etapach.

W pierwszym etapie zmiany obejmą obszary komunikacji A2A w zakresie usług RT EMIR, RT SFTR, ARM (z wyjątkiem komunikacji realizowanej w ramach SWI) oraz LEI– wdrożenie tych zmian przewidziane jest na **maj 2023 roku**.

Drugi etap obejmie modernizację w zakresie komunikacji 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, przy czym wdrożenie w tym obszarze planujemy na **kwiecień 2024 r.**
Informacje dotyczące szczegółowego harmonogramu wdrożenia wraz ze wskazaniem nowych parametrów połączeniowych do poszczególnych usług będą przekazywane Państwu odrębnie w ramach każdego z etapów.

Z poważaniem,

Sławomir Panasiuk
Wiceprezes Zarządu

Sławomir Panasiuk
Elektronicznie podpisany przez Sławomir Panasiuk
Data: 2023.03.20 15:13:26 +01'00'

Załącznik:
Specyfikacja zmian przewidzianych w ramach modernizacji komunikacji A2A

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

Załącznik: Specyfikacja zmian przewidzianych w ramach modernizacji komunikacji A2A

W ramach modernizacji kanałów komunikacyjnych służących do wymiany komunikatów w modelu A2A oraz zmian w zakresie wydawania i utrzymania certyfikatów elektronicznych, przewiduje się następujący zakres zmian.

Wydawanie certyfikatów

- Certyfikat elektroniczny, tak jak ma to miejsce obecnie, będzie służył do ustanowienia bezpiecznego szyfrowanego połączenia systemowego pomiędzy uczestnikiem a systemami informatycznymi GK KDPW. Certyfikat wystawiany będzie na dany kod instytucji uczestnika, będący czteroznakowym identyfikatorem uczestnika w danej usłudze lub usługach GK KDPW, zgodnie z ustalonym schematem.
- Obsługa certyfikatów elektronicznych, a w szczególności złożenie wniosku o jego wystawienie, pobranie certyfikatu oraz unieważnienie certyfikatu, będzie możliwa poprzez dedykowaną aplikację do zarządzania certyfikatami („Certyfikaty A2A"), udostępnioną uczestnikom w ramach Portalu usług (https://online.kdpw.pl). Dostęp do aplikacji będzie mogła 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 odbywać się będzie na jednolitych zasadach obowiązujących dla wszystkich aplikacji w ramach Portalu usług.
- Każda osoba uprawniona przez uczestnika w ramach wskazanego kodu instytucji będzie upoważniona do wnioskowania o wygenerowanie certyfikatu/certyfikatów (przy czym zakładane jest wprowadzenie ograniczenia liczby certyfikatów możliwych do wydania), aktywnych na dany kod certyfikatów. Jednocześnie możliwe będzie powtórne pobranie już wygenerowanego certyfikatu oraz unieważnienie wskazanego.
- Certyfikat będzie generowany i wydawany w oparciu o mechanizmy PKI, z wykorzystaniem algorytmu SHA-256, na bazie przekazanego przez podmiot żądania podpisanego kluczem prywatnym. Klucz prywatny będzie generowany bezpośrednio przez podmiot wnioskujący o wygenerowanie certyfikatu w ramach własnej infrastruktury, np. na bazie mechanizmów *OpenSSL*. KDPW, w ramach dedykowanej usługi zarządzania certyfikatami do komunikacji A2A, dostarczy opis procesu, który pozwoli na wykonanie wszystkich czynności przez wewnętrzne służby IT uczestnika. UWAGA: Klucz prywatny nie powinien być udostępniany osobom nieuprawnionym, w tym także nie powinien być przekazywany do KDPW.
- Wystawienie certyfikatu oraz jego udostępnienie do pobrania każdorazowo będzie wymagało akceptacji złożonego wniosku, przez KDPW, która będzie związana z przeprowadzeniem weryfikacji poprawności przekazanego żądania.

Ustanowienia połączenia A2A

- Wydany i pobrany certyfikat dla komunikacji A2A będzie wykorzystywany do komunikacji ze wszystkimi usługami, w ramach których przewidziana jest komunikacja A2A i w ramach których, dany podmiot występuje pod przypisanym do certyfikatu kodem instytucji. Certyfikat pozwoli

na ustanowienie szyfrowanej komunikacji TLS oraz uwierzytelnienie się w ramach dedykowanych dla danego kodu instytucji kanałów komunikacyjnych MQ.

- Na poziomie komunikacji A2A wprowadzona 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, w których jest udostępniana komunikacja A2A (kolejki zostaną skonfigurowane jedynie dla podmiotów faktycznie występujących i korzystających z komunikacji A2A w danej usłudze):
    - CSD – usługi podstawowe w zakresie systemu depozytowo - rozrachunkowego (dostosowanie w ramach 2go etapu wdrożenia)
    - CCP – usługi rozliczeniowe realizowane w ramach KDPW_CCP (dostosowanie w ramach 2go etapu wdrożenia)
    - EMIR – usługi raportowania do Repozytorium Transakcji EMIR (etap 1)
    - ARM – usługi raportowania do ARM (etap 1, przy czym dostosowanie komunikacji realizowanej w ramach SWI przewidziane zostało na 2 etap wdrożenia)
    - SFTR – usługi raportowania do Repozytorium Transakcji SFTR (etap 1)
    - LEI – usługi automatyzacji nadawania kodów LEI (etap 1)
    - SR – usługi Systemu Rekompensat dla uczestników bezpośrednich (dostosowanie w ramach 2go etapu wdrożenia)
- W zależności od sposobu działania usługi oraz związanych z tym oczekiwanych parametrów wydajnościowych, kolejki dedykowane komunikacji A2A będą mogły być tworzone w ramach jednego lub kilku dedykowanych kanałów komunikacyjnych. Szczegółowe parametry podłączeniowe, wraz z adresacją IP oraz nazewnictwem poszczególnych komponentów, będą prezentowane w ramach aplikacji do zarzadzania certyfikatami, udostępnionej poprzez Portal usług, wyłącznie osobom, które uzyskają dostęp do tej aplikacji na podstawie udzielonego im przez uczestnika upoważnienia.
- Nie przewiduje się zmian w obszarze funkcjonujących obecnie protokołów komunikacyjnych, dzięki czemu nie będzie potrzeby dostosowywania struktur komunikatów.

Obsługa środowisk testowych

- W ramach obsługi środowisk testowych ujednolicony zostanie model nazewnictwa poprzez wprowadzenie nazw zgodnych z obowiązującymi w Portalu usług (kanał U2A). Środowisko edukacyjne oznaczane będzie poprzez EDU, natomiast testowe dla nowych funkcjonalności, jako TST. Jednocześnie wycofane zostaną z użycia funkcjonujące obecnie nazwy TSTA oraz TSTB.
- Utrzymana zostanie zasada pojedynczego certyfikatu uprawniającego do dostępu do środowisk EDU oraz TST, przy jednoczesnym odseparowaniu komunikacji z wykorzystaniem odrębnych kolejek dla poszczególnych środowisk (także z podziałem na usługi).
- Wnioskowanie o certyfikat służący do korzystania ze środowisk testowych aplikacji GK KDPW będzie realizowane na takich samych zasadach jak wnioskowanie o certyfikat do komunikacji

w środowisku produkcyjnym, poprzez aplikację przeznaczoną do zarządzania certyfikatami w Portalu usług („Certyfikaty A2A").

Parametry techniczne połączenia

- W obszarze standardów zabezpieczeń dla połączeń telekomunikacyjnych wykorzystujących technologię VPN/IPSec przewiduje się następujące minimalne wymagania:
  - IKE Version – V2
  - Integrity (Hashing Algorithm) – SHA-256
  - Encryption Algorithm – AES-256
  - Key exchange – Diffie-Hellman Group 19

Model regulacyjny

- W ramach modelu regulacyjnego dla komunikacji A2A funkcjonować będzie odrębny regulamin ustanawiania połączeń systemowych. Obecny Regulamin dostępu do systemów informatycznych KDPW regulować będzie wyłącznie zasady dostępu do interfejsów U2A aplikacji KDPW, a w drugim etapie wdrożenia zmian systemowych, odpowiedniej zmianie będą podlegać Porozumienia SWI oraz Regulamin SWI. Taki model regulacji pozwoli na skoncentrowanie opisu zasad dostępu oraz zaadresowanie poszczególnych obszarów do podmiotów, które w praktyce będą wykorzystywać poszczególne formy komunikacji.
- W ramach wdrażania zmian dostosowywane będą również regulaminy poszczególnych usług korzystających z komunikacji A2A.