

SCP/ZW/3/2022  
CCP/ZW/233/2022

Warszawa, 25 marca 2022 r.

**Uczestnicy KDPW**  
**Uczestnicy KDPW\_CCP**  
**Uczestnicy RT EMIR**  
**Uczestnicy ARM**  
**Uczestnicy RT SFTR**  
**Podmioty zainteresowane****dot.: zmian w systemach informatycznych KDPW i KDPW\_CCP w zakresie zabezpieczeń dostępu do usług świadczonych w sieci internet**

Szanowni Państwo,

zgodnie z wcześniejszymi zapowiedziami przedstawionymi na spotkaniu w dniu 8 listopada 2021 r. dotyczącymi planowanych zmian w rozwiązaniach informatycznych GK KDPW w obszarze dostępu do usług, przedstawiamy szczegółowe informacje związane z planowanymi zmianami w obszarze:

- kanału komunikacyjnego ESDI/Web (dostosowanie do najnowszych przeglądarek) oraz
- dostępu do portalu usług <https://online.kdpw.pl> (wprowadzenie drugiego, dodatkowego składnika uwierzytelnienia).

Powyższe zmiany nie będą wymagały dostosowania w zakresie Państwa systemów informatycznych, koncentrując się przede wszystkim na interfejsach użytkownika w procesie dostępu do usług oferowanych z wykorzystaniem sieci internet.

Należy tu też podkreślić, że celem wprowadzanych zmian jest zapewnienie właściwego poziomu bezpieczeństwa na etapie dostępu do systemów i aplikacji GK KDPW, z których Państwo obecnie korzystają.

## 1. Zmiany w obszarze ESDI/Web – dostosowanie do najnowszych przeglądarek

W ramach komunikacji opartej o przekazywanie komunikatów XML, ESDI/Web stanowi narzędzie pozwalające na przesyłanie informacji o tzw. niskim wolumenie komunikatów w modelu U2A (*user to application*), z wykorzystaniem interfejsu graficznego. Dostęp do ESDI/Web przyznawany jest na podstawie wydawanych przez KDPW certyfikatów SWI, służących do uwierzytelnienia osoby przekazującej komunikat. Certyfikaty SWI są także obecnie wykorzystywane do podpisu, opartego na mechanizmach przeglądarki Internet Explorer, wycofywanej przez firmę Microsoft ze wsparcia.

Przygotowana przez KDPW modyfikacja ESDI/Web związana z wyeliminowaniem przeglądarki Internet Explorer, a tym samym funkcji podpisu, pozwoli na wykorzystanie ESDI/Web w wiodących obecnie przeglądarkach internetowych. Pozostawiona zostanie funkcja uwierzytelnienia z wykorzystaniem imiennego certyfikatu SWI (bez zmian pozostanie również proces uzyskiwania certyfikatu od KDPW). Jednocześnie, dla zapewnienia procesu weryfikacji integralności przesyłki, realizowanego obecnie przez podpis, wyznaczana będzie funkcja skrótu (tzw. *hash*) z przekazanego do przesłania pliku. Hash wyznaczany będzie z wykorzystaniem publicznych algorytmów kryptograficznych, co pozwoli na niezależne sprawdzenie integralności przesyłki przez KDPW oraz przez wysyłającego. Zmiany nie wpłyną jednak na kształt procesu wysyłania i odbierania komunikatów XML za pośrednictwem ESDI/Web.

Dodatkowo, wygaszona zostanie możliwość ustanawiania nowych połączeń z ESDI/Web poprzez REST API. Dla wszystkich Uczestników, chcących wymieniać komunikaty o wysokim wolumenie, sugerujemy wykorzystanie mechanizmów ESDK, opartych o wysokowydajną i bezpieczną infrastrukturę MQ.

Planowane zmiany w obszarze ESDI/Web, będą wymagać dokonania zmian zawartych z uczestnikami porozumień SWI oraz Regulaminu Systemu Wymiany Informacji. Aneksy do treści Porozumień SWI zostaną Państwu przedstawione do podpisania w terminie umożliwiającym ich przepracowanie oraz wejście w życie zmian porozumień w planowanym terminie wdrożenia.

**Testy:** Udostępnienie środowiska testowego i rozpoczęcie testów z Państwa udziałem przewidujemy od dnia **1 czerwca 2022 r.**

**Wdrożenie:** Rozpoczęcie produkcyjnego działania zmodyfikowanego ESDI/Web planowane jest na dzień **1 lipca 2022 r.**

## 2. Zmiany w obszarze portalu usług <https://online.kdpw.pl> - wdrożenie drugiego składnika uwierzytelnienia

W ramach podniesienia bezpieczeństwa dostępu do usług GK KDPW, mając dodatkowo na względzie wyniki analizy ryzyka dokonanej zgodnie z Wytycznymi Komisji Nadzoru Finansowego dotyczącymi zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w podmiotach infrastruktury rynku, planujemy wprowadzić wymóg uwierzytelnienia do usług udostępnianych z wykorzystaniem aplikacji w ramach portalu usług <https://online.kdpw.pl>. Powyższe

oznaczać będzie, że po wdrożeniu rozwiązania, każdy dostęp do usług na tym portalu będzie wymagać uwierzytelnienia dwoma składnikami (tzw. model MFA – *multifactor authentication*).

Wprowadzenie wymogu podania dodatkowego składnika uwierzytelnienia stanowić będzie dodatkowe zabezpieczenie pozwalające na upewnienie się, że osoba próbująca uzyskać dostęp do aplikacji GK KDPW jest tą, za którą się podaje i posiada wszelkie niezbędne atrybuty by to potwierdzić. Standardowo (na chwilę obecną) taka weryfikacja realizowana jest na bazie wskazania hasła do konta dostępowego, co stanowi tzw. atrybut wiedzy. By zwiększyć poziom wiarygodności wprowadzony zostanie drugi czynnik uwierzytelniania, który będzie bazował na tzw. atrybucie posiadania. Oznacza to, że w procesie uwierzytelnienia użytkownik będzie musiał udowodnić, że posiada dostęp do zaufanego i przypisanego mu urządzenia.

Urządzeniem zaufanym będzie :

- Aplikacja mobilna (*KDPW Group Authenticator*) instalowana na urządzeniu mobilnym działającym w oparciu o system Android lub iOS. Aplikację będzie można pobrać za darmo z autoryzowanych sklepów – Google Play (Android), App Store (iOS – Apple), a jej użycie będzie dopuszczalne jedynie na telefonach z nieprzełamanymi zabezpieczeniami systemów operacyjnych wskazanych producentów. Aplikacja mobilna, by pełnić rolę drugiego składnika uwierzytelnienia, powinna być również skojarzona z odpowiednim kontem dostępowym (tożsamością cyfrową użytkownika), co będzie dokonywane po jej zainstalowaniu przez użytkownika.

lub

- Zaufana przeglądarka internetowa, wykorzystywana na komputerze w określonej sieci i adresie IP, którą podczas logowania (po potwierdzeniu z wykorzystaniem aplikacji mobilnej) użytkownik oznaczy jako zaufaną. Wykorzystanie zaufanej przeglądarki do logowania (już po tym jak została wskazana jako zaufana) będzie weryfikowane automatycznie w procesie logowania jako dodatkowy czynnik uwierzytelnienia do wskazanego konta użytkownika.

Zarządzanie listą przypisanych do danego konta dostępowego urządzeń zdefiniowanych jako zaufane, będzie możliwe z poziomu zarządzania kontem, przy wykorzystaniu dedykowanej aplikacji <https://identity.kdpw.pl>. W ramach tej aplikacji możliwe będzie zarówno usunięcie urządzeń z listy zaufanych, jak również zweryfikowanie wszystkich operacji uwierzytelnienia przeprowadzonych z użyciem danego urządzenia. Warto w tym miejscu nadmienić, że również sam dostęp do tej aplikacji będzie wymagał użycia wieloskładnikowego uwierzytelnienia.

**Materiały:** Szczegółowe materiały, w tym instrukcje związane z obsługą aplikacji *KDPW Group Authenticator* zostały udostępnione na stronie internetowej KDPW pod adresem: <http://www.kdpw.pl/pl/MFA/Strony/default.aspx>

**Testy:** Udostępnienie środowiska testowego i rozpoczęcie testów z Państwa udziałem przewidujemy od dnia **1 kwietnia 2022 r.** Pierwszy etap testów obejmie wprowadzenie testowej strony pośredniej w ramach testowego środowiska, gdzie będzie możliwe zapoznanie się ze specyfiką działania logowania z użyciem drugiego składnika. W tym czasie portal <https://tst-online.kdpw.pl> nie będzie pozwalał na dostęp na zasadach obecnych. Począwszy od dnia **16 maja 2022 r.** wymóg podania drugiego składnika obejmie dostęp do wszystkich usług w środowisku testowym.

**Wdrożenie:** Wprowadzenie dodatkowego mechanizmu uwierzytelniania w środowisku produkcyjnym (<https://online.kdpw.pl>) oraz edukacyjnym (<https://edu-online.kdpw.pl>) planowane jest od dnia **12 września 2022 r.**

### **3. Zmiany w obszarze portalu danych <https://data.kdpw.pl> - wdrożenie nowych raportów oraz API**

W ramach rozwoju Portalu danych planujemy rozszerzyć usługę odpłatnego udostępniania przez KDPW danych referencyjnych i statystycznych GK KDPW o funkcjonalność API zgodną ze standardem OpenAPI. Dostęp do danych za pośrednictwem API stanie się dodatkową opcją dostępną w ramach subskrypcji. Można ją będzie zamówić przy tworzeniu nowej subskrypcji jak również dodać do już aktywnej. Pobieranie danych przez API możliwe będzie dla zakresu danych (pakietów), do którego dany klient ma dostęp w ramach subskrypcji płatnych. Szczegóły związane z dostępem do API oraz zasady jego działania zostaną zawarte w zaktualizowanym Regulaminie usługi.

W Portalu danych opublikowaliśmy zakładkę dedykowaną deweloperom <https://data.kdpw.pl/developers>, zawierającą specyfikacje standardu Open API, który zamierzamy zastosować do zaoferowania zautomatyzowanego, programistycznego dostępu do odpłatnych danych referencyjnych i statystycznych. Interfejs API będzie zapewniał uprawnionym klientom pobieranie wystandaryzowanych struktur danych JSON lub XML za pomocą typowych poleceń protokołu HTTP. Struktury te są już wykorzystywane przy eksporcie danych wyselekcjonowanych w ramach interaktywnego dostępu za pomocą dedykowanego GUI, wraz z wdrożeniem API będą równolegle wykorzystywane w połączeniach typu A2A (application to application).

KDPW rozwija zarówno technologiczną jak i merytoryczną zawartość Portalu w celu stworzenia serwisu odpowiadającego na zapotrzebowanie uczestników rynku kapitałowego na dane referencyjne i statystyczne. Naszym długofalowym celem jest dostarczenie Państwu kompleksowego zakresu danych referencyjnych KDPW w stopniu umożliwiającym zoptymalizowanie procesów i czynności wykonywanych w obszarze bazodanowym po Państwa stronie. W związku z powyższym wraz z powołaniem API planujemy również uruchomienie nowych raportów:

- Operacje rozrachowane w KDPW w podziale na rynek;
- Rejestracje papierów wykonane przez Agenta emisji;
- Instrukcje rozliczone przez KDPW CCP z rynku kasowego i pochodnego;
- Przyjęcie instrumentów do KDPW;
- Wycofanie instrumentów z KDPW.

O przyporządkowaniu raportów do pakietów będziemy Państwa informować za pośrednictwem Portalu danych.

**Testy:** W środowisku testowym została już udostępniona możliwość testowania API w zakresie uwierzytelniania i autoryzacji. Dostępne są także tzw. Metody API (Endpoints) służące do wywoływania zapytań i pobierania odpowiedzi w zakresie siedmiu pierwszych raportów płatnych. W pierwszej połowie kwietnia br. zostaną udostępnione do testów Metody API dla nowych raportów.

**Wdrożenie:** Implementacja API oraz nowych raportów w środowisku produkcyjnym (<https://data.kdpw.pl>) planowana jest w dniu **16 maja 2022 r.**

Z poważaniem,

Do wiadomości:

Narodowy Bank Polski  
Giełda Papierów Wartościowych w Warszawie S.A.  
BondSpot S.A.  
Izba Domów Maklerskich  
Rada Banków Depozytariuszy przy ZBP  
Urząd Komisji Nadzoru Finansowego