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/1/2024
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 przekazach 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 ujednoliceniu schematu wykorzystywanego do ich generacji. Wprowadzono również jednolite zasady związane z segregacją usług w ramach komunikacji A2A, ujednoliceniem 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, przekażemy 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

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

KDPW

Załącznik 2: Opis protokołu ESDK wykorzystywanego w ramach komunikacji A2A

Niniejszy załącznik stanowi dokumentację protokołu ESDK wykorzystywanego w części usług GK KDPW w ramach komunikacji A2A za pośrednictwem kolejek MQ.

W ramach protokołu, celem dostosowania do prowadzonych zmian w obszarze zmian certyfikatów elektronicznych (w szczególności w zakresie algorytmów kryptograficznych oraz ich wykorzystania w procesie uwierzytelniania) oraz standaryzacji zasad komunikacji A2A, wprowadzono zmiany związane z odejściem od umieszczenia w komunikacie podpisu elektronicznego. Zmiany te polegają jedynie na usunięciu z ramki pola dedykowanego dla podpisu oraz, w konsekwencji, usunięcie kontroli związanej z przekazanym podpisem. Jednocześnie integralność przesyłki będzie oparta o wbudowane mechanizmy w ramach obsługi kolejek MQ.
Pozostałe elementy protokołu pozostają bez zmian.

Informacje podstawowe

Komunikacja elektroniczna z KDPW w ramach interfejsu komunikacyjnego A2A odbywa się w oparciu o połączenia MQ zestawiane z dedykowanym menadżerem kolejek MQ. Komunikacja A2A oparta jest o spójne i jednolite zasady nawiązywania połączenia, niezależnie od protokołów wykorzystywanych w ramach poszczególnych usług. Model komunikacji A2A zakłada separację wymiany komunikatów w ramach poszczególnych usług biznesowych, co oznacza, że dla każdej z usług przewidziane zostaną odrębne kolejki MQ identyfikowane poprzez nazwę. Ponieważ zasady komunikacji A2A dopuszczają wprowadzenie na poziomie poszczególnych usług określonego (jednego lub wielu) protokołu wymiany informacji z uczestnikami, separacja obejmuje również obsługę poszczególnych protokołów w ramach pojedynczej usługi. Jako protokół komunikacyjny należy w tym wypadku rozumieć zbiór ścisłych reguł oraz formatów zapisu danych, które są wymagane celem skutecznego nawiązania komunikacji na bazie standardowego połączenia MQ.
Jednym z oferowanych w ramach komunikacji A2A protokołów jest protokół ESDK, dedykowany komunikacji z uczestnikami bezpośrednimi KDPW oraz KDPW_CCP. Protokół ten oparty jest o dedykowaną ramkę, pozwalającą na techniczne wsparcie weryfikacji poprawności komunikacji, a także potwierdzenie otrzymania komunikatu na etapie wstępnego przetwarzania. Jednocześnie protokół pozwala na przekazanie dowolnej informacji merytorycznej w oparciu o ustandaryzowane oznaczenia typu komunikatu oraz identyfikatory stron komunikacji.

Opis protokołu ESDK

Protokół komunikacyjny ESDK definiuje następujące parametry:

- format komunikatu ESDK,
- typy komunikatów ESDK,
- tryb obsługi poszczególnych typów komunikatów przez system ESDK.

Format komunikatu ESDK

Nazwa pola	Długość	Typ
Numer komunikatu	9	N
Data	10	A
Godzina	8	A
ID Adresata	10	A
ID Nadawcy	10	A
Typ komunikatu	24	A
Podtyp komunikatu	4	A
Obszar zarezerwowany	20	A
Długość danych	8	N
Dane	Długość danych	B

Typy pól:

A – znakowe
B - binarne
N – numeryczne

Każdy komunikat jest jednoznacznie i unikalnie identyfikowany na podstawie pól:

- Numer komunikatu,
- Data,
- ID Nadawcy.

Numer Komunikatu: numer kolejny komunikatu nadawcy, identyfikowanego za pomocą ID Nadawcy. Numer kolejny jest unikalny (dla danego nadawcy) w ciągu dnia oraz ciągły począwszy od 1 do n,

Data: data wygenerowania komunikatu w formacie YYYY-MM-DD,

Godzina: godzina wygenerowania komunikatu w formacie HH:MM:SS,

ID Adresata: identyfikator adresata, w formacie SDK.TTTTNN,

gdzie:
- **TTTT** - kod uczestnika,
- **NN** - numer kolejny identyfikatora dla danego uczestnika.

ID Nadawcy: identyfikator nadawcy, w formacie SDK.TTTTNN,

gdzie:
- **TTTT** - kod uczestnika,
- **NN** - numer kolejny identyfikatora dla danego uczestnika.

Typ komunikatu: określa typ komunikatu (wyrównany spacjami do prawej strony),

Podtyp komunikatu: określa podtyp komunikatu. Domyślną wartością tego pola jest ‘0000’. W komunikatach merytorycznych pierwszy znak pola może otrzymywać wartości:
- ‘T’ - dla komunikatów przekazywanych w formacie stałopolowym,
- ‘X’ - dla komunikatów przekazywanych w formacie XML,

- ‘0’ - jeżeli nie określono formatu komunikatu

Obszar zarezerwowany: obszar, który w przyszłości może zostać wykorzystany do umieszczenia dodatkowych danych w nagłówku,
Długość danych: długość pola **Dane,**
Dane: dane, które są przesyłane za pomocą komunikatu.

Typy komunikatów ESDK

Pole Typ komunikatu może przyjmować poniższe wartości:

- **esdk.acc.001.01** potwierdzenie przyjęcia komunikatu,
- **esdk.rjc.001.01** informacja o odrzuceniu komunikatu,
- **esdk.tst.001.01** komunikat weryfikujący,
- typ komunikatu merytorycznego w ramach określonej usługi.

Komunikaty, których pierwsze 4 znaki mają wartość „esdk”, w dalszej części opracowania nazywane będą komunikatami technicznymi. Pole Dane w komunikatach technicznych (z wyjątkiem komunikatu esdk.tst.001.01) ma ściśle określony format.

Struktura komunikatu esdk.acc.001.01

Struktura pola **Dane** w komunikacie typu **esdk.acc.001.01:**

Nazwa pola	Długość	Typ
Numer komunikatu	9	N
Data	10	A
ID Nadawcy	10	A
Data akceptacji	10	A
Godzina akceptacji	8	A

W ramach przekazanej struktury identyfikowany jest komunikat, który został przyjęty, wraz z informacją o dacie oraz godzinie przyjęcia.

Struktura komunikatu esdk.rjc.001.01

Struktura pola **Dane** w komunikacie typu **esdk.rjc.001.01**:

Nazwa pola	Długość	Typ
Numer komunikatu	9	N
Data	10	A
ID Nadawcy	10	A
Data odrzucenia	10	A

Godzina odrzucenia	8	A
Kod błędu	10	A
Opis błędu	256	A

Pola ***Numer komunikatu***, ***Data***, ***ID Nadawcy*** identyfikują komunikat, który został odrzucony.
Pola ***Data odrzucenia*** i ***Godzina odrzucenia*** informują o dacie i godzinie odrzucenia komunikatu.
Pola ***Kod błędu*** i ***Opis błędu*** opisują powód, z którego komunikat został odrzucony.

Sposób obsługi poszczególnych typów komunikatów

Wszystkie komunikaty odbierane przez system ESDK są weryfikowane pod kątem:

- sprawdzenia zgodności struktury komunikatu z określonym formatem,
- sprawdzenia unikalności identyfikatora komunikatu,
- dokonania kontroli charakterystycznych dla danego typu komunikatu.

W wyniku zakończenia procedury weryfikacji komunikat zostaje przyjęty lub odrzucony. Informacje o wszystkich odebranych i wysłanych komunikatach zapisywane są w rejestrze komunikatów.
W ramach obsługi komunikatów technicznych protokołu ESDK KDPW (KDPW_CCP) wykonuje następujące kontrole:

Komunikaty esdk.acc.001.01:

- jeżeli komunikat **esdk.acc.001.01** zostanie przyjęty, nie jest wykonywana żadna dodatkowa akcja,
- jeżeli komunikat **esdk.acc.001.01** zostanie odrzucony, system wysyła informację o komunikacie i wyniku jego weryfikacji do administratora systemu.

Komunikaty esdk.rjc.001.01:

Po otrzymaniu komunikatu esdk.rjc.001.01 system wysyła informację o komunikacie i wyniku jego weryfikacji do administratora systemu. W zależności od zawartości komunikatu administratorzy podejmują określone czynności wyjaśniające.

Komunikaty esdk.tst.001.01:

- jeżeli komunikat **esdk.tst.001.01** zostanie przyjęty, do nadawcy odsyłany jest komunikat **esdk.acc.001.01,**
- jeżeli komunikat **esdk.tst.001.01** zostanie odrzucony, do nadawcy odsyłany jest komunikat **esdk.rjc.001.01** informujący o odrzuceniu i jego przyczynie.

Komunikaty merytoryczne:

- jeżeli komunikat merytoryczny zostanie przyjęty jako zgodny z protokołem ESDK, do nadawcy wysyłany jest komunikat **esdk.acc.001.01**, a komunikat merytoryczny jest przekazany do przetworzenia w ramach dedykowanej usługi. W wyniku przetwarzania do nadawcy mogą być wysyłane dalsze komunikaty merytoryczne informujące o stanie oraz wynikach przetworzenia komunikatu w systemie dziedzinowym,
- jeżeli komunikat merytoryczny zostanie odrzucony jako niezgodny z protokołem ESDK, do nadawcy wysyłany komunikat **esdk.rjc.001.01** informujący o odrzuceniu i jego przyczynie, komunikat merytoryczny nie jest przekazywany do dalszego przetworzenia.

KDPW

Załącznik 3: Instrukcja pobrania certyfikatu A2A w ramach usług KDPW oraz KDPW_CCP

Niniejszy załącznik opisuje schemat certyfikatu A2A w komunikacji z usługami KDPW oraz KDPW_CCP oraz sposób jego wygenerowania i pobrania z wykorzystaniem dedykowanych aplikacji (odrębnie dla KDPW oraz KDPW_CCP) dostępnych na Portalu usług (https://online.kdpw.pl).
Po uzyskaniu dostępu do tej aplikacji osoba upoważniona przez uczestnika będzie mogła pobierać zarówno certyfikaty służące do komunikacji produkcyjnej jak i do testów. Jednocześnie aplikacja nie będzie dostępna w żadnym ze środowisk testowych Portalu usług.

Certyfikaty elektroniczne wykorzystywane w komunikacji A2A

- Do ustanowienia bezpiecznej komunikacji z usługami GK KDPW opartej o kolejki MQ w modelu A2A, wykorzystywane są certyfikaty elektroniczne oparte na kryptografii asymetrycznej w ramach tak zwanej infrastruktury klucza publicznego (PKI - *Public Key Infrastructure*).
- Certyfikat elektroniczny wystawiany jest na dany kod instytucji uczestnika i może być wykorzystany do ustanowienia komunikacji ze wszystkimi usługami, w ramach których uczestnik występuje pod tym kodem (odrębnie dla KDPW i KDPW_CCP). Certyfikat służy do ustanowienia szyfrowanego połączenia w oparciu o protokół TLS, a także do uwierzytelnienia się do odpowiedniego kanału komunikacyjnego MQ.
- W ramach komunikacji A2A z usługami KDPW ustanawia się następujący schemat certyfikatów:
    - Typ klucza (Key type) - RSA
    - Długość klucza (Key size) - 2048
    - Nazwa podmiotu X.509:
        - Organization Name (O=[A-Z0-9]{4,4}) - kod instytucji np. XXXX
        - Organizational Unit Name (OU=[PRD;TST]) - oznaczenie środowiska
        - Common Name (CN= [A-Z0-9]{4,4}+„_A2A”) - nazwa powszechna np. XXXX_A2A
- W ramach komunikacji A2A z usługami KDPW_CCP ustanawia się następujący schemat certyfikatów:
    - Typ klucza (Key type) - RSA
    - Długość klucza (Key size) - 2048
    - Nazwa podmiotu X.509:
        - Organization Name (O=[A-Z0-9]{4,4}) - kod instytucji np. XXXX
        - Organizational Unit Name (OU=[PRD;TST]) - oznaczenie środowiska
        - Common Name (CN= [A-Z0-9]{4,4}+„_CCPA2A”) - nazwa powszechna np. XXXX_CCPA2A
- Jedynie certyfikaty wygenerowane zgodne z ustalonym dla komunikacji A2A schematem i podpisane przez KDPW mogą stanowić podstawę ustanowienia komunikacji.

Opis procesu generowania certyfikatu A2A

- Certyfikat jest generowany i wydawany w oparciu o mechanizmy PKI, z wykorzystaniem algorytmu SHA-256. Proces jego uzyskania realizowany jest w kilku krokach, przy zapewnieniu bezpieczeństwa klucza prywatnego. W ramach całego procesu klucz prywatny uczestnika

wnioskującego o wystawienie certyfikatu nie jest ujawniany KDPW (powinien być zabezpieczony w ramach infrastruktury właściciela certyfikatu).

- Uzyskanie certyfikatu odbywa się na bazie przekazanego przez podmiot żądania podpisania certyfikatu (CSR - *Certificate Signing Request*), wygenerowanego i zapisanego w formacie PEM.
- Generowanie żądania podpisania certyfikatu realizowane jest bezpośrednio przez podmiot wnioskujący w ramach własnej infrastruktury, np. na bazie mechanizmów OpenSSL. Wykonanie tej czynności wymaga posiadania odpowiedniej wiedzy IT oraz dostępu do narzędzi służących do generowania kluczy prywatnych i żądań CSR.
- Tworząc żądanie podpisania certyfikatu, wnioskujący musi zadbać o jego zgodność z ustalonym schematem w obszarze typu i długości klucza oraz danych wchodzących w skład nazwy wyróżniającej (DN - *Distinguished Name*), w szczególności kodu instytucji i środowiska.
- Obsługa certyfikatów elektronicznych w zakresie złożenia wniosku o jego wygenerowanie, pobranie certyfikatu oraz unieważnienie certyfikatu, jest możliwa poprzez dedykowaną aplikację do zarządzania certyfikatami udostępnioną 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 zarządzaniem certyfikatami.
- Przekazanie żądania podpisania certyfikatu realizowane jest w postaci wniosku w aplikacji dedykowanej do obsługi certyfikatów, do którego jest ono załączane w postaci tekstowej. W ramach przygotowania wniosku aplikacja weryfikuje zgodność informacji zawartych w żądaniu ze schematem certyfikatu, w tym także z kodem instytucji, w kontekście którego jest on składany.
- Żądanie podpisania certyfikatu musi być utworzone w formacie PKCS#10 z użyciem kodowania PEM.
- Po przetworzeniu wniosku, aplikacja umożliwi pobranie wygenerowanego i podpisanego przez KDPW certyfikatu, który może zostać użyty w infrastrukturze uczestnika do ustanowienia połączenia TLS oraz uwierzytelnienia się do kanału komunikacyjnego MQ w ramach komunikacji A2A. W ramach własnej infrastruktury, wnioskujący może także połączyć otrzymany certyfikat z wygenerowanym wcześniej kluczem prywatnym w postaci kontenera PKCS#12.

UWAGA: Zachowanie ciągłości dostępu do usług w ramach kanału A2A wymaga posiadania ważnego certyfikatu. Uczestnik powinien monitorować ważność certyfikatów oraz z odpowiednim wyprzedzeniem wystąpić o wygenerowanie nowego certyfikatu. Uczestnik może też wnioskować o więcej niż jeden certyfikat dla danego kodu instytucji.

Uczestnik powinien przechowywać certyfikaty elektroniczne oraz klucze prywatne w bezpiecznym miejscu. W przypadku utraty klucza prywatnego lub w przypadku stwierdzenia jakichkolwiek naruszeń bezpieczeństwa, uczestnik jest zobowiązany do unieważnienia certyfikatu przy wykorzystaniu dedykowanej aplikacji do obsługi certyfikatów A2A. Certyfikat po unieważnieniu zostanie umieszczony na liście CRL (*Certificate Revocation List*), która jest publikowana pod adresem: http://pki.kdpw.pl/crl/kdpw-cck1.crl.

KDPW

Załącznik 4: wykorzystanie OpenSSL do uzyskania certyfikatu do komunikacji A2A

Niniejszy załącznik stanowi instrukcję w zakresie użycia narzędzia OpenSSL do wygenerowania żądania podpisania certyfikatu, niezbędnego do poprawnego złożenia wniosku w aplikacji „Certyfikaty A2A", która wraz z wdrożeniem drugiego etapu projektu będzie udostępniona uczestnikom bezpośrednim KDPW. **Analogiczna aplikacja zostanie udostępniona uczestnikom rozliczającym KDPW_CCP.** Żądanie podpisania certyfikatu powinno być generowane bezpośrednio przez podmiot wnioskujący, w jego własnej infrastrukturze, przy użyciu narzędzi kryptograficznych zgodnych z jego polityką. Tym samym polecenia opisane w załączniku należy traktować wyłącznie jako przykład wykorzystania OpenSSL, nie zaś jako wymaganie korzystania z tego konkretnego narzędzia.

UZYSKANIE CERTYFIKATU DO KOMUNIKACJI A2A

O certyfikatach dedykowanych komunikacji A2A

Certyfikat elektroniczny służący do komunikacji A2A z usługami świadczonymi przez KDPW wystawiany jest na dany kod instytucji na podstawie przekazanego żądania podpisania certyfikatu (CSR). Certyfikat wykorzystany zostanie do ustanowienia szyfrowanego połączenia w oparciu o protokół TLS, a także do uwierzytelnienia się do odpowiedniego kanału komunikacyjnego w ramach komunikacji A2A opartej o kolejki MQ.

By zapewnić bezpieczeństwo dla generowanego certyfikatu, w ramach całego procesu jego uzyskania klucz prywatny nie może opuścić infrastruktury właściciela certyfikatu. Oznacza to, że musi on być stworzony poza infrastrukturą KDPW, a sam certyfikat powinien być wygenerowany w odpowiedzi na przekazane żądanie podpisania certyfikatu, przygotowanego zgodnie z ustalonym schematem.

W ramach komunikacji A2A z usługami KDPW należy użyć certyfikatu zgodnego z następującym schematem:

- Typ klucza (Key type): RSA
- Długość klucza (Key size): 2048
- Nazwa podmiotu X.509:
  - Organization Name (O=[A-Z0-9]{4,4}) - kod instytucji np. XXXX
  - Organizational Unit Name (OU=[PRD;TST]) - oznaczenie środowiska
  - Common Name (CN= [A-Z0-9]{4,4}+„_A2A") - nazwa powszechna np. XXXX_A2A

Dla komunikacji A2A z usługami KDPW_CCP certyfikat powinien być zgodny ze schematem:

- Typ klucza (Key type): RSA
- Długość klucza (Key size): 2048
- Nazwa podmiotu X.509:
  - Organization Name (O=[A-Z0-9]{4,4}) - kod instytucji np. XXXX
  - Organizational Unit Name (OU=[PRD;TST]) - oznaczenie środowiska
  - Common Name (CN= [A-Z0-9]{4,4}+„_CCPA2A") - nazwa powszechna np. XXXX_CCPA2A

Proces może być realizowany w oparciu o szereg narzędzi implementujących algorytmy kryptograficzne i pozwalające na wygenerowanie pary kluczy w ramach architektury PKI. Przykłady wskazane w dokumentacjach KDPW odnosić się będą do narzędzi OpenSSL, dostępnych powszechnie w ramach licencji Apache, niemniej opisane do wykonania czynności mogą też być przeprowadzone z wykorzystaniem innych narzędzi.

O OpenSSL

OpenSSL (https://www.openssl.org) jest wieloplatformowym narzędziem będącym zestawem bibliotek implementujących podstawowe operacje kryptograficzne w obszarze wsparcia protokołów SSL i TLS. Jest dystrybuowany na zasadach open source w ramach licencji typu Apache, co oznacza, że może być używany nieodpłatnie do celów komercyjnych i niekomercyjnych, z zastrzeżeniem kilku warunków licencyjnych.
Pakiet instalacyjny OpenSSL może być pobrany ze strony https://wiki.openssl.org/index.php/Binaries.
Dla poprawności procesu uzyskania certyfikatu do komunikacji A2A nie ma znaczenia na jakiej platformie systemowej zostanie uruchomiony.
Wykorzystując OpenSSL należy upewnić się, że w środowisku przygotowanym do wygenerowania żądania udostępnienia podpisanego certyfikatu jest zainstalowane odpowiednie oprogramowanie kryptograficzne, oraz jest dostępne z poziomu katalogu, w którym zostanie przeprowadzona operacja, a także czy profil, z którego przeprowadzana będzie procedura posiada odpowiedni poziom uprawnień do jego użycia.

GENEROWANIE ŻĄDANIA PODPISANIA CERTYFIKATU Z WYKORZYSTANIEM OPENSSL

Generowanie z wprowadzaniem informacji w sposób interaktywny

Wygenerowanie żądania podpisania certyfikatu w sposób umożliwiający wprowadzanie danych interaktywnie wymaga wprowadzenia poniższej komendy.

```
openssl req -newkey rsa:2048 -keyout private.key -out request.csr
```

Po uruchomieniu komendy konieczne będzie podanie hasła, którym będzie zabezpieczony klucz prywatny. Ustanowione hasło będzie wymagane aby uzyskać dostęp do klucza prywatnego przy kolejnych operacjach, które będą wykonywane z jego użyciem.
Na dalszym etapie tworzenia żądania podpisania certyfikatu konieczne będzie wprowadzenie dodatkowych informacji dotyczących podmiotu, dla którego tworzony będzie certyfikat. Jest istotnym, aby dane wprowadzane w odpowiednie pola były zgodne z przyjętym schematem. Wartości pól spoza schematu mogą być pominięte, co w przypadku OpenSSL oznacza wprowadzenie znaku kropki („.”).
W przypadku CSR wypełnienie pól przedstawia się następująco:

- Country Name (2 letter code) - „.”
- State or Province Name (full name) - „.”
- Locality Name (e.g., city) - „.”
- Organization Name (e.g., company) - kod instytucji np. XXXX
- Organizational Unit Name (e.g., section) - kod środowiska (PRD lub TST)

- Common Name (e.g., server FQDN) - nazwa powszechna np. XXXX_A2A
- Email Address - „.”
- A challenge password - „.”
- An optional company name - „.”

Po zakończeniu, gotowe do przesłania żądanie zostanie zapisane we wskazanym przy wywołaniu komendy pliku CSR – w przedstawionym przykładzie będzie to plik „request.csr”. Zawartość pliku CSR powinna być przekazana do KDPW w treści wniosku, składanego z wykorzystaniem aplikacji „Certyfikaty A2A”.

Generowanie automatyczne, za pomocą pełnej komendy

Jedną z dostępnych opcji podczas tworzenia żądania podpisania certyfikatu jest podanie wszystkich niezbędnych informacji w samym poleceniu za pomocą opcji -subj dostępnej dla komendy OpenSSL. W ramach wartości dla opcji możliwe jest wskazanie informacji wymaganych w ustalonym schemacie certyfikatu. W przypadku certyfikatu do komunikacji A2A w ramach usług KDPW dane powinny być wskazane w następujący sposób.

```
-subj "/O=XXXX/OU=TST/CN=XXXX_A2A"
```

Pełna komenda utworzenia żądania podpisania certyfikatu przyjmuje zatem następującą postać.

```
openssl req -newkey rsa:2048 -subj "/O=XXXX/OU=TST/CN=XXXX_A2A" -keyout
private.key -out request.csr
```

Po wywołaniu komendy należy wprowadzić hasło do zabezpieczenia klucza prywatnego, a następnie je potwierdzić. W efekcie klucz prywatny zostanie zakodowany z użyciem wprowadzonego hasła, będzie ono wymagane w przypadku konieczności użycia klucza prywatnego.
By wskazać hasło bezpośrednio w komendzie utworzenia pliku CSR należy wywołać poniższą komendę (w przedstawionym przykładzie ciąg znaków „123456789” stanowi hasło).

```
openssl req -newkey rsa:2048 -subj "/O=XXXX/OU=TST/CN=XXXX_A2A" -passout
pass:123456789 -keyout private.key -out request.csr
```

Po zakończeniu, gotowe do przesłania żądanie zostanie zapisane we wskazanym przy wywołaniu komendy pliku CSR – w przedstawionym przykładzie będzie to plik „request.csr”. Zawartość pliku CSR powinna być przekazana do KDPW w treści wniosku, składanego z wykorzystaniem aplikacji „Certyfikaty A2A”.

Pobranie treści żądania podpisania certyfikatu

Uzyskanie certyfikatu podpisanego przez Centrum Autoryzacyjne KDPW realizowane jest poprzez aplikację „Certyfikaty A2A” dostępną w Portalu Usług, gdzie po uwierzytelnieniu oraz wybraniu właściwego kodu instytucji, istnieje możliwość złożenia stosownego wniosku. W treści wniosku (wykorzystując przewidziane do tego okno tekstowe) należy wkleić treść wygenerowanego pliku CSR.

By pobrać treść pliku można posłużyć się dowolnymi metodami. W zależności od preferencji, można otworzyć plik CSR w dowolnym edytorze tekstowym, po czym skopiować zawartość do składanego w aplikacji wniosku. Można też wyświetlić treść pliku CSR korzystając z linii poleceń i następujących komend:

- w systemie Windows

```
more .\request.csr
```

- w systemie Linux

```
cat ./request.csr
```

Wyświetlona zawartość pliku CSR wygląda podobnie do przykładu wskazanego poniżej. Co istotne, kopiując zawartość należy uwzględnić znaczniki początku i końca żądania.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICdTCCAV0CAQAwMDENMAsGA1UECgwEWFhYWDEMMAoGA1UECwwDVFNUMREwDwYD
VQQDDAhYWFhYX0EyQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKyl
otU7qeztCrG23DjSrJlPGdVwtj5Ikdid7BDgWTNMji+6rgYHosMtXT+slmMH3oSp
ryN9eKl1Ci3L5VdTuye7/qaPsAoHnTmdH8gSu67RVeRmqZkYfjorPQBWF+cKGhca
RMy2z0AoUfHEa51KV/lWBRo/ulm0a0V1E7sRrS/Fk/7pCJ3Vbh9KsrZIxNa4ZLux
tRYFOEoBBJ/Nri7mPOm+39hx98nR6czEOcBtGJ8KKPyZXbluZs5j1Gh7qGBO8h/h
0BM5RESMcls56qpANq21jrxT7shK1il6lbsxgGHCIJKqbzk9sPPkHYBpfeDZOb4p
L1KWU03PiLlOHoBdR88CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQAdDCLkd+LD
4MjLWdejk0L5KCC6S97M1sagfBeWBgxcv0ncfSx8laKMb9sjFWcQW75io/E5fH69
nosWQNAWdQO37vB4cRr3ihlLTrks3VqVD7OYowTEK735VYYXM9wBnhmYbY0o9SnN
UnWx/RIise1eokj9BFbW07EOZ5MiwcZ4PTVBk1AKRBHzPVNM4bOifrJskoQ8+S4g
+Jx3LTBSJ5VZBARDxKYWnkYSFV4krUa+Xlmj89G1LP3jern6j8SCJVX3tf7s+a+o
1COGvZ576NA4n1bHLfbKU4KMJiIRcpz8iW+gkJSdz1nwr00LhwVAKxjtHPMET4s+
4L1nSrXwUx24
-----END CERTIFICATE REQUEST-----
```

POBRANIE WYGENEROWANEGO CERTYFIKATU

Po złożeniu wniosku o wydanie podpisanego przez KDPW certyfikatu oraz jego przetworzeniu przez KDPW, w aplikacji „Certyfikaty A2A" udostępniony zostanie certyfikat w formacie PEM. Może on zostać pobrany po wybraniu opcji „Zapisz", dostępnej dla aktywnych certyfikatów w widoku z listą wydanych dla danego kodu instytucji certyfikatów.

Pobrany certyfikat stanowi parę z kluczem prywatnym wygenerowanym wraz z tworzeniem pliku CSR, dlatego, zwłaszcza przy generowaniu większej liczby certyfikatów, warto zadbać o to, by nie utracić tego powiązania. Można też powiązać certyfikat z jego kluczem prywatnym w pliku PFX (format PKCS#12)

Dalsze czynności związane z wykorzystaniem certyfikatu zależą od wewnętrznej infrastruktury instytucji, dla której certyfikat został wygenerowany.

Połączenie certyfikatu i klucza prywatnego z wykorzystaniem formatu PKCS#12

Format PKCS #12 (PFX) przechowuje i certyfikat i klucz prywatny w jednym zaszyfrowanym pliku. By utworzyć certyfikat w tym formacie po jego pobraniu z KDPW (format PEM) można posłużyć się poniższą komendą.

```
openssl pkcs12 -inkey private.key -in certificate.pem -export -out certificate.pfx
```

Jeśli utworzony wcześniej klucz prywatny został zakodowany z użyciem hasła, do wykonania operacji niezbędne będzie jego podanie. Dodatkowo, w trakcie tworzenia pliku PFX możliwe będzie wprowadzenia hasła zabezpieczającego dane w tworzonym pliku.

WERYFIKACJA

Przedstawione w tym rozdziale komendy OpenSSL pokazują sposoby weryfikacji poprawności wytworzonych danych. Wykonywanie tych operacji nie jest niezbędne do uzyskania certyfikatu A2A, niemniej pozwoli na ustalenie przyczyn ewentualnych błędów w trakcie przeprowadzenia procesu.

Weryfikacja poprawności przygotowanego żądania podpisania certyfikatu

```
openssl req -text -in request.csr -noout -verify
```

Komenda pozwoli zweryfikować podpis w pliku CSR, a także wybrany algorytm i zawartość pól wprowadzonych w ramach ustalonego przez KDPW schematu.

```
Certificate request self-signature verify OK
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: O = XXXX, OU = TST, CN = XXXX_A2A
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ac:a5:a2:d5:3b:a9:ec:ed:0a:b1:b6:dc:38:d2:
                    ac:99:4f:19:d5:70:b6:3e:48:91:d8:9d:ec:10:e0:
                    96:63:07:de:84:a9:af:23:7d:78:a9:75:0a:2d:cb:
                    51:f1:c4:6b:9d:4a:57:f9:56:05:1a:3f:ba:59:b4:
                    ... (dalsza część nie została pokazana)
```

Jeśli podpis nie zostanie zweryfikowany poprawnie (wprowadzone zostały modyfikacje w zawartości pliku CSR) lub pozostałe dane nie będą odpowiadały wymaganemu przez KDPW schematowi, wniosek o wydanie certyfikatu zostanie odrzucony.

Weryfikacja zgodności kluczy

Weryfikacja zgodności plików wytwarzanych w ramach procesu uzyskiwania certyfikatu może być przeprowadzona poprzez sprawdzenie zgodności klucza publicznego, wyodrębnionego z każdego z plików. Jeśli dla wszystkich plików klucz publiczny jest zgodny oznacza to, że są one zgodne i dotyczą jednego certyfikatu. Ten sposób może też pomóc ustalić, czy klucz prywatny odpowiada certyfikatowi, w przypadku utraty pewności co do ich powiązania.
By uprościć proces porównania kluczy prywatnych można skorzystać z funkcję skrótu SHA-256 dla wyodrębnionych wartości.

By obliczyć funkcję skrótu dla poszczególnych plików z użyciem OpenSSL należy użyć następujących komend:

- SHA-256 klucza publicznego na podstawie klucza prywatnego

```
openssl pkey -pubout -in .\private.key | openssl sha256
```

- SHA-256 klucza publicznego na podstawie żądania podpisania certyfikatu (CSR)

```
openssl req -pubkey -in .\request.csr -noout | openssl sha256
```

- SHA-256 klucza publicznego na podstawie uzyskanego certyfikatu

```
openssl x509 -pubkey -in .\certificate.pem -noout | openssl sha256
```

Funkcje powinny być wywoływane niezależnie.
Wynikiem każdej z funkcji jest informacja o wartości skrótu obliczonej dla klucza publicznego wyodrębnionego z każdego z plików. Wynik przyjmuje następującą postać.

```
SHA2-256(stdin)=
afd5b3b3739493c373024416a60d42676227007a6c62dcdfa72a96cfda3edb5c
```

W przypadku stwierdzenia różnic w prezentowanej wartości, zestaw plików nie reprezentuje danych dotyczących tego samego certyfikatu. W takich wypadkach rekomenduje się powtórne wygenerowanie certyfikatu.