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.