PolishAPI

Rekomendacje oraz podstawowe założenia do testowania interfejsu dedykowanego

Dokument opracowany przez Grupę Projektową ds. PolishAPI

8 lipca 2019
Wersja 1.0

Opis czynności do wykonania po stronie TPP, potwierdzających poprawne przetestowanie API ASPSP zgodnego z PSD2:

1. Nawiązanie połączenia za pomocą certyfikatu transportowego Qualified Website Authentication Certificate (QWAC) zgodnego normą EIDAS*.
2. Podpisywanie wysyłanych zapytań do ASPSP. Do generacji sygnatury JWS wykorzystywany jest certyfikat Qualified Electronic Seal Certificate (QsealC)*.
3. Weryfikacja certyfikatów QWAC i QSealC ASPSP*:
    a. weryfikacja daty ważności certyfikatu;
    b. weryfikacja czy CA wystawiające certyfikat jest na głównej liście TSL (zawężonej do CA posiadających akredytację do wystawiania QWAC i/lub QsealC);
    c. weryfikacja pełnej ścieżki certyfikatu;
    d. sprawdzenie czy certyfikat nie jest unieważniony poprzez sprawdzenie listy CRL;
    e. (opcjonalnie) weryfikacja poprawnej obsługi odrzuceń przez API żądań, jeżeli atrybuty PSD2 w certyfikacie nie uprawniają TPP do korzystania z konkretnej usługi.
4. Weryfikacja czy podpis w sygnaturze JWS jest autentyczny, czy został rzeczywiście wygenerowany przez ASPSP, do którego zostało wysłane zapytanie.
5. Ustanowienie sesji komunikacyjnej z Bankiem i uzyskanie tokenów OAuth2 poprzez wykonanie kroków:
    a. wysłanie zapytania za pomocą metody /authorize, gdzie po pozytywnej weryfikacji w odpowiedzi zostanie zwrócony adres, pod którym jest wystawiony serwis bankowości internetowej, w której PSU się uwierzytelnia;
    b. przekierowanie PSU na otrzymany adres i po pozytywnym uwierzytelnieniu i przekierowaniu na redirect_uri pozyskanie parametru auth_code;
    c. obsługa odmowy udzielenia zgody przez PSU i innych błędów w bankowości internetowej (zwrotne przekierowanie przeglądarki PSU do TPP);
    d. uzyskanie access_token i refresh_token po wywołaniu metody /token i przekazaniu posiadanego auth_code.
    e. użycie refresh_token w celu pozyskania nowego access_token;
    f. (opcjonalnie) wykorzystanie exchange_token w celu pozyskania nowego access_token o zmienionym zakresie zgód.
6. Weryfikacja poprawnej obsługi odrzuceń przez API żądań w związku z brakiem lub wygaśnięciem zgód.
7. Weryfikacja poprawnej obsługi odrzuceń przez API żądań AIS, które przekraczają określone przez dyrektywę limity dzienne.

8. Wykonanie wszystkich metod PolishAPI, których użycie planuje TPP (i ma do nich uprawnienia poprzez nadane role PSD2) i które są udostępniane przez danego ASPSP. Weryfikacja powinna w szczególności dotyczyć następujących obszarów:
    a. sprawdzenie czy w żądaniach wysyłane są wszystkie pola wymagane przez ASPSP w wykorzystywanych metodach;
    b. generacja unikalnego requestId;
    c. obsługa stronicowania odpowiedzi;
    d. (opcjonalnie) obsługa kontekstu klienta korporacyjnego;
    e. (opcjonalnie) usługi callback.
9. Środowisko sandboxowe ASPSP powinno zapewnić TPP komunikację za pomocą testowych certyfikatów QWAC i QSealC zgodnych z normą EIDAS w przypadku, kiedy TPP nie posiada jeszcze własnych certyfikatów produkcyjnych.

UWAGA (*) Użycie i weryfikacja certyfikatów EIDAS jest krokiem opcjonalnym w przypadku środowiska testowego (sandboxowego), może też być testowane niezależnie od metod biznesowych (5-8).

W kontekście użycia certyfikatów EIDAS, zaleca się, aby ASPSP w swojej dokumentacji uwzględniły następujące aspekty:

1. Zdefiniowanie maksymalnego rozmiaru nagłówka http, jaki zostanie obsłużony,
2. W kontekście użycia nagłówka x5u oczekiwane jest, że podany w nim adres url będzie obsługiwał bezpieczne połączenie,
3. Oczekiwaną wartość nagłówka „kid” podpisu,
4. Przykłady wyliczenia podpisu wraz z oczekiwanymi polami.