PolishAPI

Rekomendacje oraz podstawowe założenia do przygotowania interfejsu awaryjnego

Dokument opracowany przez Grupę Projektową ds. PolishAPI

8 lipca 2019
Wersja 1.0

Spis treści

Spis ilustracji

1 Wstęp i zastrzeżenia

Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (RTS) zobowiązuje dostawców usług płatniczych prowadzących rachunek płatniczy (ASPSP) do opracowania środków awaryjnych w zakresie specjalnego interfejsu dostępowego. Środki awaryjne obejmują m.in. opis dostępnego interfejsu awaryjnego (*fall-back*).

Ani druga dyrektywa w sprawie usług płatniczych (PSD2), ani RTS nie przesądzają szczegółowo pożądanego kształtu i sposobu funkcjonowania interfejsu awaryjnego. Ograniczone wymogi regulacyjne w tym zakresie wynikają z art. 33 ust. 5 RTS.

Niniejsze *Rekomendacje oraz podstawowe założenia do przygotowania interfejsu awaryjnego* stanowią propozycję wspólnego, uniwersalnego podejścia do wdrożenia interfejsu awaryjnego, wykorzystującego dotychczasowe osiągnięcia polskiego sektora bankowego i płatniczego oraz najlepsze praktyki rynkowe.

Rekomendacje i opisy założeń zawarte w niniejszym dokumencie nie mają, w żadnym zakresie i wymiarze, charakteru wiążącego. Nie są to także jedyne możliwe rozwiązania, które są dopuszczalne w świetle wymogów prawnych. ASPSP mogą, wedle własnego uznania i przeprowadzonej oceny ryzyka oraz na własną odpowiedzialność, podjąć decyzję o stosowaniu przedstawionych tutaj rekomendacji i opisów założeń, w całości lub części. Niniejszy dokument nie stanowi także opinii prawnej.

Rekomendacje i opisy założeń zawarte w niniejszym dokumencie prezentują pogląd wypracowany w ramach prac grupy projektowej przy Związku Banków Polskich.

2 Założenia

1. Pierwszym etapem procesu jest weryfikacja certyfikatu QWAC użytego do zestawienia połączenia oraz certyfikatu pieczęci QSealC TPP.
2. Weryfikacja certyfikatów opiera się na weryfikacji certyfikatów QWAC i QSealC umieszczonych w nagłówkach. W ramach weryfikacji dokonywana jest analiza ważności certyfikatu, jego struktury oraz uprawnień TPP do usług PSD2. UWAGA: weryfikacja certyfikatu pieczęci z uwagi na potencjalny znaczny wpływ na wydajność usługi bez krytycznego wpływu na jej bezpieczeństwo, może być uznana za opcjonalną.
3. Uwierzytelnienie klienta opiera się o mechanizm przekierowania do infrastruktury ASPSP (*redirection*).
4. Realizacja usług następuje po uwierzytelnieniu PSU oraz przekazaniu tokena lub identyfikatora sesji, aby umożliwić TPP realizację usługi na interfejsie klienckim wg wybranej przez ASPSP metody.
5. Realizacja usługi AIS bez udziału PSU nie jest objęta niniejszą rekomendacją, a jej udostępnienie zależy od indywidualnej decyzji ASPSP.

3 Usługa inicjacji płatności (PIS) – opis procesu

Uwaga, wprowadzenie danych przelewu może nastąpić przed uwierzytelnieniem lub po uwierzytelnieniu PSU. Będzie to skutkowało koniecznością wykorzystania innego procesu i innej jego obsługi.

1. PSU uruchamia aplikację webową TPP używając przeglądarki WWW. W tym kroku PSU może wprowadzić także dane przelewu.
2. Serwer TPP nawiązuje połączenie z domeną fallback.<bank>.pl. TPP przekazuje parametr *tpp_redirect_uri* zawierający adres serwera TPP, do którego w kolejnych krokach procesu będą realizowane przekierowania przeglądarki PSU.
3. Weryfikacja certyfikatu QWAC użytego do zestawienia połączenia oraz certyfikatu pieczęci QSealC TPP*.
4. Jeżeli weryfikacja TPP na podstawie przekazanych certyfikatów zostanie zakończona powodzeniem generowany jest *token**, który zostanie wykorzystany przez ASPSP do potwierdzenia realizacji usługi. Dodatkowo zostanie zwrócony URL prowadzący do adresu, pod którym znajduje się *endpoint* ASPSP. W przypadku negatywnej weryfikacji TPP połączenie zostanie odrzucone.
5. TPP przekierowuje przeglądarkę PSU na stronę bankowości elektronicznej ASPSP w oparciu o URL otrzymany w poprzedzającym kroku.
6. PSU uwierzytelnia się na stronie bankowości elektronicznej ASPSP podając swoje dane logowania. Dodatkowo, do bankowości elektronicznej ASPSP jest przekazany *token* wygenerowany uprzednio, zawierający m.in. potwierdzenie poprawnej weryfikacji certyfikatów TPP.
7. ASPSP zwraca do TPP *token.*
8. Na podstawie parametru *tpp_redirect_uri*, następuje przekierowanie PSU na stronę aplikacji TPP.
9. Serwer TPP ponownie łączy się z ASPSP w celu pobrania danych sesji, w kontekście której zostanie nawiązanie połączenie.
10. ASPSP przekazuje dane sesji.
11. TPP łączy się z bankowością elektroniczną w kontekście PSU, wykorzystując otrzymane wcześniej dane sesji w celu realizacji akcji w imieniu PSU. Ten krok może obejmować wprowadzenie danych przelewu.

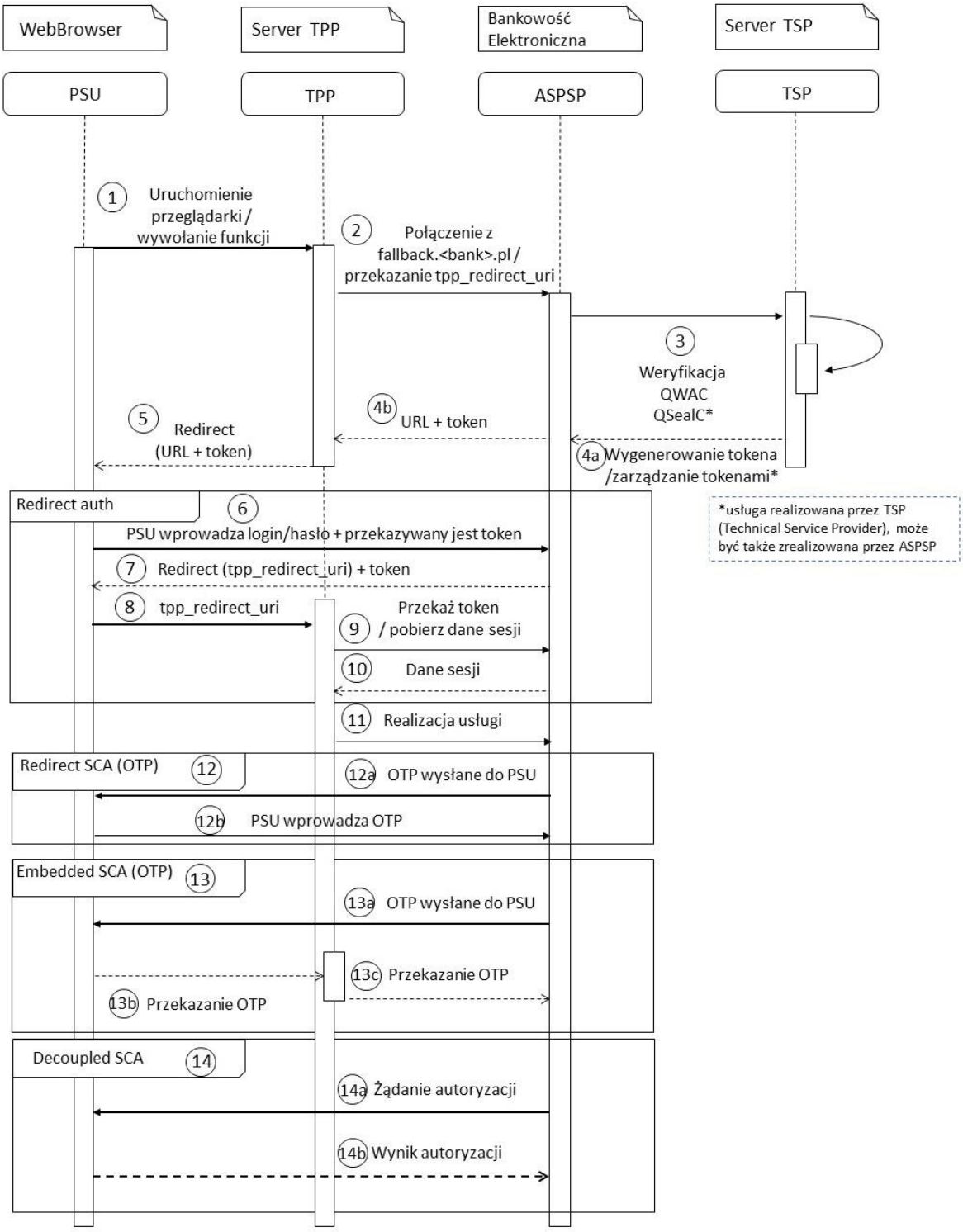
Drugi faktor uwierzytelnienia jest wprowadzany w oparciu o trzy dopuszczalne metody, opisane w punktach 12, 13 i 14:

12. Metoda *redirection*, np. z wykorzystaniem OTP (*One-time password*):
    a. ASPSP generuje OTP i przekazuje go PSU istniejącym kanałem (np. za pośrednictwem SMS);
    b. PSU potwierdza żądanie / autoryzuje transakcję w interfejsie ASPSP. Ta metoda jest transparentna z pkt. widzenia TPP.
13. Metoda *embedded*, np. z wykorzystaniem OTP (*One-time password*):
    a. ASPSP generuje OTP i przekazuje go PSU istniejącym kanałem (np. za pośrednictwem SMS);
    b. PSU wpisuje OTP w aplikacji TPP;
    c. TPP używa przekazanego kodu do autoryzacji żądania / transakcji.
14. Metoda *decoupled* (np. za pośrednictwem osobnej aplikacji ASPSP na urządzeniu mobilnym):

a. ASPSP generuje żądanie autoryzacji i wysyła komunikat *push* do urządzenia mobilnego;

b. PSU potwierdza żądanie / autoryzuje transakcję. Ta metoda jest transparentna z punktu widzenia TPP.

***usługa realizowana przez TSP (Technical Service Provider), może być także zrealizowana przez ASPSP**



***Ilustracja 1:** Proces inicjacji płatności*

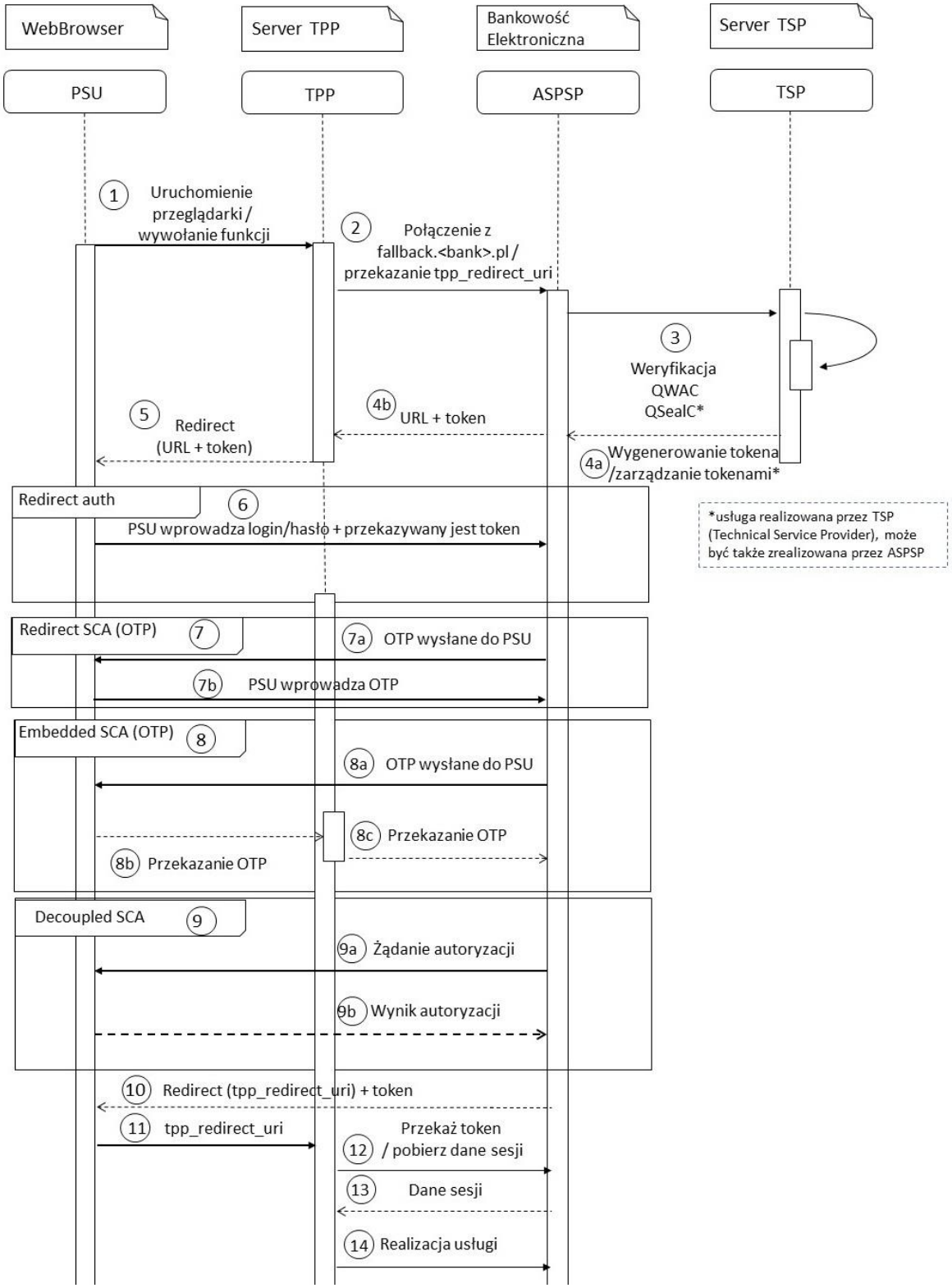
4 Usługa dostępu do informacji o rachunku (AIS) – opis procesu

1. PSU uruchamia aplikację webową TPP używając przeglądarki WWW.
2. Serwer TPP nawiązuje połączenie z domeną fallback.<bank>.pl. TPP przekazuje parametr *tpp_redirect_uri* zawierający adres serwera TPP, do którego w kolejnych krokach procesu będą realizowane przekierowania przeglądarki PSU.
3. Weryfikacja certyfikatu QWAC użytego do zestawienia połączenia oraz certyfikatu pieczęci QSealC TPP*.
4. Jeżeli weryfikacja TPP na podstawie przekazanych certyfikatów zostanie zakończona powodzeniem generowany jest *token**, który zostanie wykorzystany przez ASPSP do potwierdzenia realizacji usługi. Dodatkowo zostanie zwrócony URL prowadzący do adresu, pod którym znajduje się *endpoint* ASPSP. W przypadku negatywnej weryfikacji TPP połączenie zostanie odrzucone.
5. TPP przekierowuje przeglądarkę PSU na stronę bankowości elektronicznej ASPSP w oparciu o URL otrzymany w poprzedzającym kroku.
6. PSU uwierzytelnia się na stronie bankowości elektronicznej ASPSP podając swoje dane logowania. Dodatkowo, do bankowości elektronicznej ASPSP jest przekazany *token* wygenerowany uprzednio, zawierający m.in. potwierdzenie poprawnej weryfikacji certyfikatów TPP.

Drugi faktor uwierzytelnienia jest wprowadzany w oparciu o trzy dopuszczalne metody, opisane w punktach 11, 12 i 13:

7. Metoda *redirection*, np. z wykorzystaniem OTP (*One-time password*):
   a. ASPSP generuje OTP i przekazuje go PSU istniejącym kanałem (np. za pośrednictwem SMS);
   b. PSU potwierdza żądanie / autoryzuje transakcję w interfejsie ASPSP. Ta metoda jest transparentna z pkt. widzenia TPP.
8. Metoda *embedded*, np. z wykorzystaniem OTP (*One-time password*):
   a. ASPSP generuje OTP i przekazuje go PSU istniejącym kanałem (np. za pośrednictwem SMS);
   b. PSU wpisuje OTP w aplikacji TPP;
   c. TPP używa przekazanego kodu do autoryzacji żądania / transakcji.
9. Metoda *decoupled* (np. za pośrednictwem osobnej aplikacji ASPSP na urządzeniu mobilnym):
   a. ASPSP generuje żądanie autoryzacji i wysyła komunikat *push* do urządzenia mobilnego;
   b. PSU potwierdza żądanie / autoryzuje transakcję. Ta metoda jest transparentna z pkt. widzenia TPP.
10. ASPSP zwraca do TPP *token.*
11. Na podstawie parametru *tpp_redirect_uri*, następuje przekierowanie PSU na stronę aplikacji TPP.
12. Serwer TPP ponownie łączy się z ASPSP w celu pobrania danych sesji, w kontekście której zostanie nawiązanie połączenie.
13. ASPSP przekazuje dane sesji.
14. TPP łączy się z bankowością elektroniczną w kontekście PSU wykorzystując otrzymane wcześniej dane sesji w celu pobrania danych w imieniu PSU.

***usługa realizowana przez TSP (Technical Service Provider), może być także zrealizowana przez ASPSP**



Ilustracja 2: Proces dostępu do informacji o rachunku (z udziałem PSU)