

## PSD2

CaixaBank, SA opracowuje adaptację interfejsu oddziału w Polsce, aby zapewnić dostęp zewnętrznym dostawcom usług płatniczych (TPP i CBPII), aby mogli oni korzystać z takiego interfejsu do uwierzytelniania i komunikacji z użytkownikami usług płatniczych (PSU).

Rozwiązanie jest opracowywane w celu spełnienia wymagań i funkcjonalności określonych w Rozporządzeniu RTS, w ustalonym terminie 14 września 2019 r. (Rozporządzenie Delegowane (UE) 2018/389 w sprawie regulacyjnych standardów technicznych w zakresie silnego uwierzytelniania klienta oraz powszechnych i zabezpieczonych otwartych standardów komunikacji" („Rozporządzenie RTS”).

— Rozporządzenie RTS wymaga stosowania certyfikatów eIDAS w celu identyfikacji TPP. Specyfikacje eIDAS są zawarte w normie ETSI TS 119 495.

Wszelkie żądania dotyczące kont PSU wymagają podpisu w celu zapewnienia identyfikacji TPP. Podpisy HTTP zapewniają podejście uwierzytelniające i umożliwiają weryfikację, czy komunikacja między klientem a serwerem nie została naruszona. Podejście to jest standaryzowane przez IETF.

Aby poprawnie podpisać żądanie, TPP będzie musiał podjąć następujące kroki:

1. **Użycie certyfikatu podpisującego:** Wymagany jest certyfikat eIDAS QSEAL wydany przez kwalifikowanego dostawcę usług zaufania.
2. **Tworzenie podsumowania:** Należy wygenerować skrót nagłówek HTTP żądania zakodowany w formacie Base64. Dopuszczalne metody algorytmu haszującego wymagają potwierdzenia i ostatecznego zdefiniowania elementów tworzenia podsumowania.
3. **Wiersz podpisu:** Należy utworzyć wiersz podpisu zawierający datę i nagłówki podsumowania. Nadal nie wiadomo, czy do wiersza zostaną dodane inne nagłówki.
4. **Podpis kluczem prywatnym:** Wiersz podpisujący uzyskany w poprzednim kroku zostanie podpisany kluczem prywatnym.
5. **Tworzenie nagłówka podpisu:** Nagłówek podpisu dodany do żądania będzie zawierał podpisany ciąg znaków uzyskany w kroku 4. Ostateczne elementy nagłówka podpisu wymagają jeszcze zdefiniowania.