# Opis interfejsu awaryjnego (fallback)

## wdrożonego w Credit Agricole Bank Polska S.A.

Version 1.0

14.09.2019

Spis treści

# 1. Kontekst

Interfejs awaryjny (fallback) jest udostępniany przez Credit Agricole Bank Polska S.A. zgodnie z wymaganiami opisanymi w Artykule 33 Rozporządzenia Delegowanego Komisji (UE) 2018/389 dotyczącego silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (dalej: RTS). Rozwiązanie umożliwia uprawnionym podmiotom (Third Party Providers – dalej: TPP), korzystanie z serwisów internetowych udostępnianych klientom Banku (CA24 i CA24 Biznes) w celu realizacji usług wprowadzonych zgodnie z Dyrektywą Parlamentu Europejskiego I Rady (UE) 2015/2366 w sprawie usług płatniczych w ramach rynku wewnętrznego (…) (dalej: PSD2): dostępu do informacji o rachunku, inicjowania płatności, usług płatniczych dostawców wydających instrumenty płatnicze oparte na karcie .

# 2. Udostępnienie interfejsu awaryjnego

Zgodnie z Artykułem 33 RTS, interfejs awaryjny udostępniany jest jedynie w przypadku wystąpienia problemów z dostępnością lub nieodpowiednią wydajnością interfejsu specjalnego (API XS2A). W momencie przywrócenia dostępności API XS2A dostęp do interfejsu awaryjnego jest wyłączany.

O każdym uruchomieniu i wyłączeniu dostępu do interfejsu awaryjnego Bank powiadamia przez zamieszczenie komunikatu w Serwisie API Portal (https://apiportal.credit-agricole.pl).

# 3. Opis interfejsu awaryjnego

## 3.1. Adresy dostępowe serwisu

Interfejs (interfejsy) zapasowe udostępniane są pod dedykowanymi adresami:

- Dla klientów indywidualnych oraz małych i średnich przedsiębiorstw:

*https://ca24-fallback.credit-agricole.pl/*

- Dla obsługi klientów korporacyjnych:

*https://ca24biznes-fallback.credit-agricole.pl/*

Oba adresy, pod którymi dostępny jest interfejs awaryjny, zabezpieczone są certyfikatami QWAC zgodnymi z normą ETSI TS 119 495 pozwalającymi na jednoznaczną identyfikację Banku. Certyfikaty te posiadają poniższe cechy („Subject”):

```
CN=ca24-fallback.credit-agricole.pl
O=Credit Agricole Bank Polska S.A.
2.5.4.97=PSDPL-PFSA-6570082274
OU=DDUiT
L=Wrocław
ST=dolnosląskie
C=PL
```

```
CN=ca24biznes-fallback.credit-agricole.pl
O=Credit Agricole Bank Polska S.A.
2.5.4.97=PSDPL-PFSA-6570082274
OU=DDUiT
L=Wrocław
ST=dolnośląskie
C=PL
```

## 3.2. Zasady dostępu

Każdy podmiot chcący rozpocząć korzystanie z interfejsu awaryjnego musi posiadać uprawnienia w zakresie świadczenia którejkolwiek z usług: PIS, AIS, CAF oraz identyfikować się ważnym, kwalifikowanym certyfikatem uwierzytelniania witryn internetowych (QWAC), wydanym zgodnie z Artykułem 34 RTS oraz normą ETSI TS 119 495.

Zgodnie z artykułem 41 ust. 5 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, PSD2, Bank zastrzega sobie możliwość odmówienia dostawcy świadczącemu usługę dostępu do informacji o rachunku lub dostawcy świadczącemu usługę inicjowania płatności dostępu do danego rachunku płatniczego z obiektywnie uzasadnionych i należycie udokumentowanych względów związanych z nieuprawnionym lub nielegalnym dostępem do rachunku płatniczego przez tego dostawcę świadczącego usługę dostępu do informacji o rachunku lub tego dostawcę świadczącego usługę inicjowania płatności, łącznie z nieuprawnionym lub nielegalnym zainicjowaniem transakcji płatniczej.

## 3.3. Uruchomienie interfejsu awaryjnego

W celu uruchomienia interfejsu awaryjnego należy zestawić bezpieczne połączenie z wykorzystaniem, identyfikującego podmiot TPP, certyfikatu QWAC, z odpowiednimi dla danej grupy klientów, adresami (https://ca24-fallback.credit-agricole.pl/ lub https://ca24biznes-fallback.credit-agricole.pl/).

Przy nawiązaniu połączenia z domeną fallback następuje weryfikacja certyfikatu QWAC strony łączącej się do serwisu – jego ważności, zgodności z normą ETSI dotyczącą certyfikatów używanych do identyfikacji podmiotów rynku PSD2 oraz weryfikacja uprawnień.

Po pozytywnej weryfikacji TPP, następuje przekierowanie na stronę pozwalającą na uwierzytelnienie klienta (Payment Services User – dalej: PSU).

## 3.4. Uwierzytelnienie klienta (PSU)

Zgodnie z Artykułem 33 ust. 4 RTS, Bank pozwala TPP na „korzystanie z interfejsów udostępnionych użytkownikom usług płatniczych na potrzeby uwierzytelnienia i komunikacji" wraz ze wszystkimi regułami i sposobami uwierzytelniania dostępnymi dla tych użytkowników.

## 3.5. Ograniczenia interfejsu awaryjnego

Interfejs awaryjny od strony funkcjonalnej odpowiada interfejsom udostępnianym użytkownikom Banku co najmniej w zakresie:

- ✓ Dostępu do informacji (w tym historii transakcji) o rachunkach zakwalifikowanych przez bank jako płatnicze
- ✓ Możliwości zlecania płatności z ww. rachunków.

Ze względu na brak możliwości technicznych weryfikacji zgody, operacje dostępu do rachunku lub zlecania płatności wykonywane są bezpośrednio, TPP ma obowiązek działać w granicach zgody udzielonej mu przez użytkownika.

Wszystkie operacje wykonywane w interfejsie awaryjnym są przez bank rejestrowane, a zlecane transakcje płatnicze oznaczane właściwym identyfikatorem TPP (pozyskanym z certyfikatu podmiotu łączącego się z interfejsem awaryjnym – atrybut „organizationIdentifier").

### 3.6. Komunikaty błędów interfejsu awaryjnego

Interfejs awaryjny oprócz standardowych komunikatów przekazywanych użytkownikom (PSU), może zwrócić poniższe, wynikające z jego specyfiki, błędy:

- ✓ **401** Unauthorized – Bank nie może zweryfikować poprawności certyfikatu. Błąd może wynikać z braku certyfikatu, wykorzystania niekwalifikowanego certyfikatu, niezgodności certyfikatu z normą ETSI, jego unieważnienia lub wygaśnięcia.
- ✓ **403** Forbidden – Bank nie może zweryfikować uprawnień TPP. Błąd może wystąpić w przypadku blokady TPP dokonanej przez Bank ze względu z nieuprawnionym lub nielegalnym dostępem do rachunku płatniczego, jak również w przypadku braku uprawnień do działania w charakterze TPP.
- ✓ **410** Gone – Interfejs awaryjny jest wyłączony. Błąd zwracany w okresach, w których interfejs awaryjny jest niedostępny. Oznacza to, że funkcjonalność interfejsu specjalnego XS2A została przywrócona.

## 4. Obowiązki TPP wynikające ze stosowania interfejsu awaryjnego

Udostępniając interfejs awaryjny, Bank wskazuje na obowiązki nałożone na TPP, wynikające z jego stosowania, w tym zwłaszcza:

- ✓ Wprowadzenie niezbędnych środków w celu zapewnienia, aby TPP nie miał dostępu do danych, nie przechowywał danych ani nie przetwarzał ich w innych celach aniżeli świadczenie usług wyraźnie zleconych przez użytkownika usług płatniczych,
- ✓ Dalsze przestrzeganie obowiązków wynikających odpowiednio z art. 66 ust. 3 i art. 67 ust. 2 PDS2, w tym w szczególności uzyskiwanie dostępu wyłącznie do informacji dotyczących wyznaczonych rachunków płatniczych i związanych z nimi transakcji płatniczych, a także nieżądania szczególnie chronionych danych dotyczących płatności,
- ✓ Obowiązek rejestrowania danych, do których TPP uzyskał dostęp za pośrednictwem interfejsu Banku na potrzeby swoich użytkowników usług płatniczych, i na wniosek bez zbędnej zwłoki przedstawiania plików rejestrów właściwemu organowi krajowemu.
- ✓ Obowiązek odpowiedniego informowania Banku o korzystaniu z interfejsu awaryjnego.

Ze względu na brak możliwości, w ramach standardowych adresów udostępnianych przez Bank użytkownikom usług płatniczych (PSU), identyfikacji dostawców usług płatniczych, o których mowa w art. 30 ust. 1 RTS niedozwolone jest korzystanie przez TPP bezpośrednio z adresów ***https://ca24.credit-agricole.pl/*** oraz ***https://ca24biznes.credit-agricole.pl/.***

Próby pozyskania informacji przez interfejsy użytkownika dostępne przez wskazane wyżej adresy będą mogły być przez Bank blokowane oraz zgłaszane do odpowiednich organów nadzoru.