Contingency Interface Description

implemented at Credit Agricole Bank Polska S.A.

Table of Contents

1. Context

A contingency (fallback) interface is made available by Credit Agricole Bank Polska S.A. in line with the requirements of Article 33 of the Commission Delegated Regulation (EU) 2018/389 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (hereinafter: the RTS). The solution makes it possible for authorised entities (Third Party Providers, hereinafter: TPP) to use online services available to the Bank's Customers (CA24 and CA24 Biznes) to carry out the following services introduced in accordance with Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market (…) (hereinafter: PSD2): account information service, payment initiation service, and payment services offered by payment service providers issuing card-based payment instruments.

2. Granting Access to Contingency Interface

In accordance with Article 33 of the RTS, a contingency interface is only made available if there are problems with the availability or performance of the special interface (API XS2A). Once API XS2A becomes available again, access to the contingency interface shall be disabled.

The Bank shall place relevant information in the API Portal Service (https://apiportal.credit-agricole.pl) each time access to the contingency interface is made available or disabled.

3. Contingency Interface Description

3.1. Dedicated Addresses

Fallback interface(s) have dedicated addresses:

- For individual customers and small and medium-sized enterprises:

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

- For corporate clients:

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

Both addresses of the contingency interfaces are protected with QWAC certificates compliant with the ETSI TS 119 495 standard, certificates which enable the Bank to be identified unequivocally. The aforementioned certificates have the following features ("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. Rules for Access

Any entity that wants to use the contingency interface must be authorised to provide any of the following services (PIS, AIS, CAF) and hold a valid qualified website authentication certificate (QWAC) issued in line with Article 34 of the RTS and the ETSI TS 119 495 standard.

In accordance with Article 41.5 of the Payment Services Act (PSD2) of 19 August 2011, the Bank reserves the right to deny an account information service provider or payment initiation service provider access to a given payment account if there are justified and documented reasons related to unauthorised or illegal access to a payment account by that account information service provider or payment initiation service provider, including unauthorised or illegal payment service initiation.

3.3. Initiating the Contingency Interface

To start up the contingency interface, a secure connection with the address corresponding to a given group of customers (https://ca24-fallback.credit-agricole.pl/ or https://ca24biznes-fallback.credit-agricole.pl/) needs to be established, using the QWAC certificate identifying the TPP.

When connection with the fallback domain is initiated, the QWAC certificate of the website connecting with the service is verified for its validity and compliance with the ETSI standard for certificates used for the purposes of identifying PSD2 market entities. Authorisations are also verified.

If the outcome of verification is positive, the TPP is redirected to the website that makes it possible to authenticate the customer (Payment Services User, hereinafter: the PSU).

3.4. Customer (PSU) Authentication

In accordance with Article 33.4 of the RTS, the Bank allows the TPP to "use interfaces that have been made available to payment service users for the purposes of authentication and communication", including all rules and methods of authentication that are available to such users.

3.5. Contingency Interface Restrictions

When it comes to functionalities, the contingency interface at least corresponds to interfaces made available to the Bank's users as regards:

- ✓ Access to information (including the history of transactions) about accounts classified by the Bank as payment accounts
- ✓ The option of ordering payments using the aforementioned accounts.

Since it is not technically feasible to verify a consent, actions that relate to getting access to an account, or ordering a payment, are carried out directly, and the TPP is obliged to act as permitted by the user when s/he gave his/her consent.

The Bank records all actions carried out with the use of the contingency interface, and payment transactions are tagged with the appropriate TPP ID (obtained from the certificate of the entity connecting with the contingency interface – the "organizationIdentifier" attribute)

3.6. Contingency Interface Error Messages

Apart from standard messages sent to users (PSUs), the contingency interface may send the following error messages arising from its specific nature:

- ✓ **401 Unauthorized** – The Bank cannot verify the authenticity of the certificate. The error may be caused by the absence of a certificate, the use of an unqualified certificate, a certificate being non-compliant with the ETSI standard, or an invalidated or expired certificate.
- ✓ **403 Forbidden** – The Bank cannot verify the TPP's authorisations. The error may occur due to a TPP having been blocked by the Bank due to unauthorised or illegal access to a payment account, but also in the case of an entity not being authorised to act as a TPP.
- ✓ **410 Gone** – The contingency interface has been disabled. This error message is sent when the contingency interface is unavailable. This means that the special XS2A interface is operational again.

4. TPP's Duties Arising from the Use of a Contingency Interface

While launching the contingency interface, the Bank wishes to remind TPPs of their duties arising from the use of the interface, including in particular:

- ✓ To adopt all necessary measures to ensure that the TPP neither has access to data nor stores or processes such data for any other reason than providing the services it has been explicitly instructed to provide by a payment service user,
- ✓ To continue to comply with the requirements arising from Article 66.3 and Article 67.2 of PSD2, including in particular only accessing information from designated payment accounts and associated payment transactions, and not requesting sensitive payment data,
- ✓ The duty to record data accessed by the TPP via the Bank's interface for their payment service users, and to disclose register files to the competent national authority without unnecessary delay, if so requested.
- ✓ The duty to inform the Bank, in an appropriate manner, that the TPP is using the contingency interface.

Since it is not possible to identify payment service providers referred to in Article 30.1 of the RTS directly with the use of standard addresses made available by the Bank to payment service users (PSUs), TPPs are prohibited from using the addresses ***https: //ca24.credit-agricole.pl/*** and ***https: //ca24biznes.credit-agricole.pl/*** directly**.**

Attempts to obtain information via user interfaces available at the aforementioned addresses may be blocked by the Bank, and they may be reported to relevant supervisory authorities.