CREDIT AGRICOLE BANK POLSKA S.A.

Documentation summary of XS2A interface

implemented at Credit Agricole Bank Polska SA

Version 2.0

2020-10-17

Table of contents

1 PSD2. General information

1.1 Definitions

The terms used herein with an initial capital shall carry the meaning assigned to them below.

AIS – the Account Information Service is an online service consisting in the provision of consolidated information on one or more payment accounts held by a payment service user with another payment service provider or with more than one payment service provider.

API – the Application Programming Interface is a set of rules that describes how applications and systems can communicate with one another.

API XS2A – a programming interface made available by the Bank to enable authorised entities to carry out automated communication with the Bank with respect to the provision of PIS, AIS and CAF services.

ASPSP – the Account Servicing Payment Service Provider.

AST – Agreed Service Time is monthly availability, i.e. the total time of operation up to the total time in which the service should operate, counted on a monthly basis in hours of service provision.

Bank – Credit Agricole Bank Polska S.A.

CAF – a service consisting in Confirming of the Availability of Funds necessary to carry out a card transaction in the payment account.

Working day – a day from Monday to Friday, excluding Saturdays, Sundays and public holidays of the Republic of Poland.

PSD2 Sandbox – a separate IT environment in the IT system of the Bank, via which a User has the opportunity to independently test the API XS2A provided by the Bank.

PIS – the Payment Initiation Service is a service consisting in initiating a payment at the request of a payment service user in relation to a payment account held with another payment service provider.

Polish API – an interface standard developed by the Polish Bank Association's Polish API working group.

PSD2 (Payment Service Directive) - Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

PSU (Payment Services User) – a natural or legal person using a payment service as a payer, payee or payer and payee.

Website – the API Portal Website.

TPP– Third Party Providers providing payment services of PIS, AIS or CAF types pursuant to the Payment Services Act of 19 August 2019.

User – a natural person, a legal person or an organisational unit without legal personality, which is granted legal capacity by law, having a registered account in the API Portal Website.

1.2 Business context

API (Application Programming Interface) is a term used to describe a set of technologies allowing for data exchange between IT solutions.

Modern banks use complex and secure IT systems to provide services such as enabling access to information on payment accounts and the possibility of making payments from such accounts. In order to be able to build advanced solutions tailored to the needs of the business (corporate clients), banks have for years been offering various types of API to allow access to their services.

So far, services provided by banks in the form of API have not been regulated and have depended mainly on the bank's strategy. The entry into force of the Payment Services Directive (PSD2) standardises the market in this respect by imposing on banks an obligation to make payment account details available to authorised entities and by making it possible for such entities to initiate payments from such accounts in the way specified in the directive. At the same time, PSD2 does not impose any restrictions on banks as to the number of services they will make available in addition to those listed as mandatory in the Directive.

1.3 Possible ways of integration

The basic ways of integration include:

- Individual integration with selected business partners through dedicated interfaces,
- Universal integration with intermediaries (TPP) offering services using or interfacing with electronic banking, through a unified interface.

So far, the basic method of integration has been for the bank to make the original set of APIs available. Using this type of interface it is possible to create business solutions that support direct communication with the bank. Dedicated APIs also constitute the communication core for payment systems already existing on the market.

The entry into force of the PSD2 regulation introduces a second method of integration based on a unified API. In the case of the Polish market, the PolishApi standard is the implementation (operationalisation) of the PSD2 directive.

1.4 Security

The security of services available thanks to PSD2 is ensured on several levels.

In formal terms, in order to become a TPP, it is not enough to merely create a service compatible with XS2A interfaces. As a rule, TPP is subject to notification and verification, which, if positive, results in the issuance of an appropriate certificate, which also determines the roles in which a given TPP may operate.

In technical terms, in order to enable communication with banks, TPP entities must be properly authenticated before access to the XS2A interface is granted to them, so as to ensure a high level of protection against both unauthorised entities impersonating TPP and unauthorised escalation of the authorisation level by TPPs with legal access to the XS2A interface. Authentication is based on public key certificates in the mutual authentication process using the TLS 1.2+ protocol.

TPP authorisation in the model used by the Bank must be based on the RBAC (Role Based Access Control) model, in which the level and scope of access to particular API resources depends on the PolishAPI user's role.

Regardless of the PSU authentication mechanism (customer, end-user) used in AIS and PIS services, the assumption is that this process ends with an access token being issued by ASPSP. Operations ordered by TPPs are always performed with the use of a valid access token.

2 Implementation of PSD2 API requirements at Credit Agricole Bank Polska S.A.

2.1 General information

The API XS2A made available by the Bank is a product that enables TPP to initiate payments, collect data on payment accounts maintained by the Bank and confirm the availability of the amount in the account to the extent required by the amended Payment Services Act and specified by the PolishAPI standard.

https://polishapi.org/dokumentacja-standardu/;

Technical documentation for services with instructions for their provision is available on the API Portal Website. Access to the documentation is possible after registering and properly filling in the application form available on the Website. On the basis of such an application the Bank decides to grant additional rights to the applicant. Access is granted to Users who represent the TPP and payment service providers that have applied for TPP status (that have submitted an application for a relevant permit/registration with the competent authorities).

If the decision is positive, the Bank will make documentation related to API XS2A available on the Website within 5 working days from the date on which the User submitted a complete application.

Note

Any entity wishing to start using the API to provide services implemented in accordance with the PSD2 Directive to the Payment Services Act, must first be registered in at least one register in a European Union Member State in the role in which it wishes to operate within this process. It must also have a valid certificate for the purposes of being identified by banks during the communication process. Such certificates are issued by qualified trust service providers.

2.2 Security

The solution made available by the Bank ensures:

- The highest level of security in the process of authentication and authorisation of a TPP request through the use of tokens and qualified certificates,
- Confidentiality of transmitted data, guaranteed by the use of the secure SSL/TLS protocol to secure the transmission channel,
- Authorisation of consents for calling PolishAPI services, executed on the basis of authorisation flows defined in PolishAPI.
- Storage of customer consents in an appropriately secured authorisation database.
- Verification of each request sent by TPP within the scope of AIS/PIS/CAF services defined in the PolishAPI, in terms of consents given by customers and in terms of signatures contained in messages in order to ensure non-repudiation.

2.3 Scope of services

API XS2A made available by the Bank was prepared in accordance with the specification of the PolishAPI version 2.1.1. and subsequently was upgraded to version 3.0.

This solution makes it possible:

- For the customer to authorise the operations performed by the TPP regarding the following:
    - The right to download a list of accounts
    - The right to download information on one or more accounts indicated by the customer
    - The right to initiate a single payment or a batch payment and to download information on the status of initiated single payments and batches.

- To download information on payment accounts regarding the following:
    - List of all accounts of a customer
    - Detailed information about a given account
    - Information on transactions divided into types
    - Detailed information on a specific transaction

- To handle payment orders regarding the following:
    - Domestic payment orders
    - International payment orders
    - Payment orders to the tax office
    - Ordering payment batches of a certain type
    - Downloading information about the status of single payments, a number of payments in one request and about payment batches
    - Deletion of payment orders with a future date

- To handle inquiries about the availability of funds in a payment account.

2.4 API XS2A variants

The Bank provides two variants of the API focused on access to two different business segments:

- Services for individual customers and small and medium enterprises –API XS2A Retail https://xs2a.credit-agricole.pl/CaPolishAPI/prod/individual/,
- Services for corporate clients – API XS2A Corpo https://xs2a.credit-agricole.pl/CaPolishAPI/prod/corporate/.

3 Test environment

The Bank provides an environment allowing for tests of API XS2A functionality (PSD2 Sandbox).

3.1 General Information

The PSD2 Sandbox is a separate IT environment in the IT system of the Bank, via which a Registered User has the opportunity to independently test API XS2A provided by the Bank.

The data available in the PSD2 Sandbox is statistical data prepared especially for testing purposes. The data makes it possible to test all the services made available in line with the scenarios prepared by the Bank.

The PSD2 sandbox does not implement all the security functions provided in the real environment, such as verification of a qualified TPP (with special attributes of the PSD2 role), transaction limits, customer rights, anti-fraud mechanisms etc.

3.2 Access to the environment

Access to the PSD2 Sandbox is given together with access to API XS2A documentation.

Authentication is based on certificates of the public key in the Mutual authentication process using the TLS 1.2+ protocol. In the case of the Sandbox, TPP uses a non-qualified certificate that complies with the “ETSI TS 119 495” technical specification.

3.2.1 Certificates

- Certificates used for authentication of clients using PSD2 Sandbox services are issued by the Bank.
- Certificates for testing purposes are issued for a period of 6 months (in the case of entities that document their application for TPP status) and for a period of 12 months in the case of entities with TPP status.
- Certificates allow you to test all services regardless of the actual role of TPP.

3.2.2 Issuing a certificate

In order to gain access to the PSD2 Sandbox you need to:

- Apply for a certificate when sending an application for access to documentation

or

- Fill in a special form available on the Website,
- Send the completed and signed document by e-mail to HYPERLINK "mailto:apiportal@credit-agricole.pl"

If the User meets all the formal requirements, the Bank will deliver the test certificate within 5 working days from the date of submission of the completed application by the User.

3.2.3 Cancelling a certificate

A certificate issued by the Bank for testing purposes may be cancelled due to:

- The User being deprived of access to PSD2 documentation resulting e.g. from the organisation the User represents losing TPP status;
- Detection of a violation by the User of PSD2 security rules (e.g. attempts to break security mechanisms),
- Detection of a certificate having been compromised,
- Other reasons – at the request of the registered User of the PSD2 Sandbox.

3.3 Security rules

It is forbidden to use the PSD2 Sandbox in any other way than that described in the documentation. In particular, it is forbidden to test the security mechanisms implemented by the Bank in an unauthorised manner and attempts to break them.

The Bank is authorised to use technical and organizational measures to prevent misuse of the Sandbox.

The Bank may block the User’s access to the Sandbox in the event of justified suspicion of fraud or a threat to the security of the Sandbox related to any unauthorised use of the Sandbox by the User.

Responsibility for potential violations of generally applicable law and of the rights of third parties, resulting from use of the Service, in particular behaviour inconsistent with its test purpose, rests fully with the User using the Service.

3.4 Technical conditions and availability

The Bank assumes the availability of the Sandbox (AST) will be at a level of 90% per calendar month.

The number of inquiries from one user may be limited in a given time unit (the Bank guarantees it will process not less than 10 inquiries per second).

Due to the test nature of the environment, its performance does not correspond to that of the real environment and cannot be used as a basis for claims; also, the environment may not be used for performance tests.

4 Support

The Bank provides technical and business support on working days from 9.00 am to 5.00 pm.

Requests should be e-mailed in Polish or English to:

- API_PSD2@credit-agricole.pl – for errors and technical issues connected with the API and the PSD2 Sandbox, including problems with the availability of the interfaces
- apiportal@credit-agricole.pl – for other questions connected with the solution implemented by Credit Agricole, including those connected with the documentation and certificates issued by the Bank for the purposes of carrying out tests via the Sandbox

The Bank will do its utmost to ensure that the user receives a response to their enquiry within no more than 10 working days.

5 Logotypes

As regards payment initiation services and account information services, Credit Agricole Bank Polska S.A. (the “Bank”) makes its trademarks available in the form published on the API Portal (https://apiportal.credit-agricole.pl) to ensure that services provided by the Bank as the trademark owner can be identified.

The Bank gives its consent for its trademark to be used for information purposes connected with providing PIS and AIS services without the need to obtain a licence for the use thereof as long as it is necessary for a third party (being a payment service provider referred to in Article 2.4(b)- 2.4(f) of the Payment Services Act) to be able to provide services. The Bank does not give its consent for its trademark to be used if the trademark has been modified in any way, including in particular if its colour, proportions or shape have been changed or if the trademark has been combined with another trademark. The only admissible form in which the trademark can be used is that specified in the Bank's access interface documentation.

At the same time, the Bank hereby warns that using the Bank's trademark in any way that suggests that there is a link between the Bank and a given TPP, or that the TPP's services are promoted via the use of the Bank's trademark, is prohibited.