Imex banka d.d. PSD2 Interface

Table of Contents

1. Interface Functionality

A. On-boarding

Access to the Payment Initiation Service API is controlled through the general on-boarding/enrollment flow: the API is only accessible to valid TPPs, who have completed the enrollment in order to upload and verify their qualified certificates. By accessing the API, you confirm that you already have status as an authorized TPP - or (for sandbox access only) that your application has been submitted to a local National Competent Authority (NCA) and is pending approval. Only TPPs who can document their authorization status are eligible to receive support.

1. A third-party provider (TPP) signs up to https://test1.evolva.cloud/imexbanka/app
2. TPP receives a verification email
3. TPP receives an email notification of successful registration
4. TPP logs into https://psd2test.imexbanka.hr:443 to access the certificate, the API key and the secret to connect to the API sandbox
5. TPP tests the API

TPP starts using the production endpoint

B. Account Information Access Consent

A PSU initiates the account information consent transaction in order for the TPP to be able to perform the following transactions:

1. Query for a list of reachable accounts once;
2. Query for balances on the reachable accounts once or multiple times;
3. Query for payment transactions on the reachable accounts once or multiple times.

The following is applicable to the account access consent process:

- If the balance or transaction information access is granted for an account, the right to access this account’s detailed information is assumed.
- For multi-currency accounts, the account access can be granted on either the account or sub-account level.
- The multiple access term length is limited to the number of days specified by the PSD2 requirements.
- The PSU can limit the number of corresponding transactions per day.

The ASPSP will reject the request if:

- the TPP cannot be identified correctly at the XS2A interface or if it does not have the **AISP** role.

Sample sequence:

1. The PSU requests the TPP to get account information;
2. The TPP queries ASPSP for account information;
3. The ASPSP directly authenticates the PSU with SCA;
4. The ASPSP provides the PSU’s access token to the TPP;
5. The TPP pulls the account information.

C. Payment Initiation

Only PSUs can initiate payment transactions through a TPP with the Payment Initiation Service Provider (**PISP**) role. Similar to account information retrieval, payments must be accepted with the use of strong customer authentication (SCA). SCA can be used for each specific payment, but it is also possible to initiate multiple payments, and then use a signing-basket to authorise multiple payments simultaneously.
The ASPSP will reject the request if:

- the TPP cannot be identified correctly at the XS2A interface or if it does not have the **PISP** role;
- the PSU has not consented to the corresponding transaction of the TPP.

In case of creation of a single payment or consent not requiring any additional data to be submitted, the ASPSP can initiate a redirect to process SCA immediately after the transaction initiation. In this case, the ASPSP will create all the corresponding authorisation sub-resources pointed to by the hyperlinks provided in the response. Refer to API Steering for details.

i. Bulk Payments

All payment transactions composing a bulk payment are based on the same payment product and withdraw funds from the same account of the PSU.

ii. Recurring Payments

The actual booking is similar to the processing of recurring payments initiated by a corresponding standing order and determined by frequency, duration, funds availability and validity.

D. Payment Cancellation

Only PSUs can initiate payment cancellation process through a TPP with the Payment Initiation Service Provider (**PISP**) role.

- A cancellation request shall be processed for a payment initiated earlier by the same TPP.
- Cancelling a bulk payment will affect all included payments.
- Cancelling a recurring payment will affect only future payments.

The ASPSP will reject the request if:

- the TPP cannot be identified correctly at the XS2A interface or if it does not have the **PISP** role;
- the PSU has not consented to the corresponding transaction of the TPP.

E. Availability of Funds

TPPs can request confirmation of funds availability on a specific account belonging to a PSU as a “YES”/”NO” response. No further detail about the account is returned.
The transaction flow is as follows:

- The PSU initiates a transaction at the PSU-TPP interface, for example, at a checkout;
- The TPP verifies funds availability by requesting through the XS2A interface.

The ASPSP will reject the request if:

- the TPP cannot be identified correctly at the XS2A interface or if it does not have the **PIISP** role;
- the PSU has not consented to the corresponding transaction of the TPP.

F. Transaction grouping – Signing Baskets

TPPs may choose to group multiple transactions into a signing basket. In order for a set of transactions to form a basket, all of them need to satisfy the following conditions:

- The transaction has been initiated through a PIS.
- The transaction is a transaction of the use case "Establish account information consent" through an AIS.
- The transaction has not been fully authorized yet, i.e. at least the authorisation of one PSU shall be missing.

The grouping is possible only by request from the PSU through the PSU-TPP interface.
The ASPSP will reject the grouping if:

- the TPP cannot be identified at the XS2A interface;
- the TPP does not have the necessary roles corresponding to the transactions to be grouped.

The ASPSP may require that SCA complies with all requirements of the Commission Delegated Regulation [RTS] for all transactions included in the basket.

G. List of Accessible Accounts

The ASPSP specifies the base set of online accessible payment accounts as defined in articles 65, 66, 67 of PSD2. The TPP receives only corresponding accounts numbers without any additional information. The TPP may obtain more detailed account information through further API calls, provided that the PSU has granted this kind of access while establishing the account information consent.
The transaction is initiated by the TPP and does not have to be initiated by the PSU. The PSU must have granted the corresponding consent earlier.
The ASPSP will reject the request if:

- the TPP cannot be identified correctly at the XS2A interface or if it does not have the **AISP** role;
- the PSU has not consented to the corresponding transaction of the TPP.

H. Query Accessible Account Details

The TPP may obtain account balance and transaction information, provided that the PSU has granted this kind of access while establishing the account information consent.
The transaction is initiated by the TPP and does not have to be initiated by the PSU.
Following is a list of types of account information available for query:

- Type and name of the account;
- Aliases used to address the account;
- Balances;

- Hyperlinks to the account resources.

The ASPSP will reject the request if:

- the TPP cannot be identified correctly at the XS2A interface or if it does not have the **AISP** role;
- the PSU has not consented to the corresponding transaction of the TPP.

i. Query Account Balances

The TPP can query for each accessible account balance in a separate request.
For multi-currency account, the ASPSP returns a list of all corresponding sub-accounts' balances and their currency codes.

ii. Query Account Transaction Information

The TPP can query for transactions on each accessible account in a separate request.
For multi-currency account, the ASPSP returns a list of transactions on all corresponding sub-accounts and their currency codes.

2. Extended Scope Functionality

TPPs with additional access rights have the ability to execute an extended set of transactions in order to enhance their functionality, improve user experience and simplify interaction with the ASPSP.
To enable this functionality, the TPP needs to get authorization by using an API key and secret issued by the ASPSP allowing REST API requests to an extended set of published endpoints.

A. Enhancements to a TPP-Only Transaction Flow

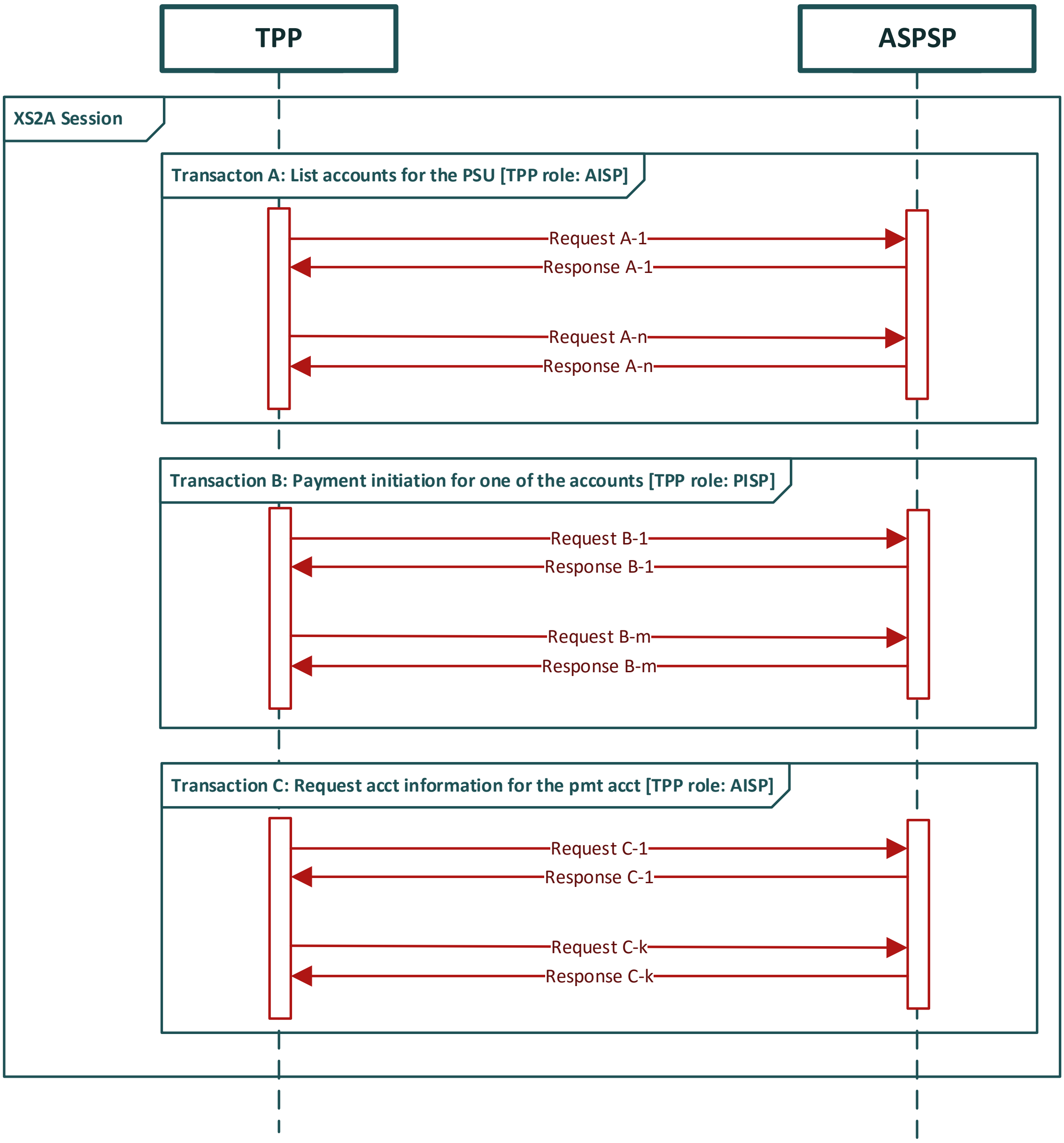
1. availability of funds functionality (a PIISP-scope) to non-PIISPs;
2. PSU initiated available accounts list update enhancing the TPP-to-PSU interface;
3. Per-PSU consent review
   a. when performed at the PSU-to-TPP interface, allows consent enabling/disabling;
   b. when executed by a TPP's reporting software, allows for anonymous statistical analysis used for market research and analytical tooling.
4. The ASPSP exposes its functionality as AISP, PIISP or PISP.

B. Additional Functionality

1. detailed per-TPP transaction listing to be used as an enhancement to the TPP's in-house reporting;
2. ability to configure default payment methods for TPPs adding extra value to the TPPs that are clients of the ASPSP.

3. Session Support

The ASPSP provides support for sessions in order for the TPPs with multiple roles to execute their transaction sequences requiring the TPU’s account information consent verification and the SCA without interruptions.


TPP
ASPSP
XS2A Session
Transacton A: List accounts for the PSU [TPP role: AISP]
Request A-1
Response A-1
Request A-n
Response A-n
Transaction B: Payment initiation for one of the accounts [TPP role: PISP]
Request B-1
Response B-1
Request B-m
Response B-m
Transaction C: Request acct information for the pmt acct [TPP role: AISP]
Request C-1
Response C-1
Request C-k
Response C-k

In the above example, transactions A, B and C can belong to different TPP roles but still share a common security context and the PSU consent reference.

4. TPP Identification

The ASPSP performs both the transport (QWAC profile) and the application (QSealC profile) layer TPP verification:

a. the TPP must use its own qualified certificate for website authentication (QWAC) to identify itself and establish the TLS connection;
b. the TPP must use its own qualified certificate for electronic seals (QSealC) to sign all of its requests to the ASPSP.

For detailed information refer to Draft ETSI TS 119 495, Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificates Profiles and TSP Policy Requirements under the Payment Service Directive 2015/2366/EU, V1.1.2 (2018-07)

The ASPSP will reject a transaction if the TPP cannot be identified correctly at the XS2A interface or if the transaction is not provisioned by the set of roles specified in the certificate. Refer to articles 65, 66 and 67 of ***Directive (EU) 2015/2366 of the European Parliament and of the Council on Payment Services in the Internal Market, published 25 November 2016***.

5. Authentication and Authorisation with OAuth 2.0

- The PSU authentication exchange results in receiving an access token to be used towards XS2A with the requests that follow later.
- The authorisation process allows the payment initiations and the consent related interactions as follows:
  1. The PIS flow:
     a. the payment initiation endpoint receives payment data;
     b. the ASPSP gets the payment authorised with "Authorisation Code Grant" and with the corresponding "scope" attribute;
     c. the ASPSP initiates the payment
  2. The AIS flow:
     a. the consent endpoint receives consent data from the AIS;
     b. the ASPSP gets the consent by the PSU to grant the AIS access with "Authorisation Code Grant" and with the corresponding "scope" attribute;
     c. the TPP can use the access token the "accounts" endpoint until the token expires

The OAuth is configured as follows:

- Response type: "code"
- Grant types: "authorization_code" and "refresh_token"
- As a mitigation technique for a possible code substitution attacks, the Proof Key for Code Exchange (PKCE) is used.

Refer to the following standards and specifications for more information:

- OAuth 2.0: https://tools.ietf.org/html/rfc6749
- The "BEARER" authorization schema: https://tools.ietf.org/html/rfc6750
- PKCE: https://tools.ietf.org/html/rfc7636
- JWT: https://tools.ietf.org/html/rfc7519
- It is strongly recommended to follow the security best practices

6. Operational Rules

A. Business Data Format

i. Payment Data

JSON as defined in ***NextGenPSD2 XS2A Framework, Implementation Guidelines, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, version 1.3, published October 2018***

ii. Account Information

JSON as defined in ***NextGenPSD2 XS2A Framework, Implementation Guidelines, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, version 1.3, published October 2018***

B. Restrictions

Article 68 of ***Directive (EU) 2015/2366 of the European Parliament and of the Council on Payment Services in the Internal Market, published 25 November 2016*** specifies limits of the use of the payment instrument and of the access to payment accounts by the ASPSP. The ASPSP is provided the functionality to enable and disable TPP access to its services.

C. Payment Transaction Management

PSUs have access to their payment records through the PSU to ASPSP interface with the following functionality:

1. Revocation of payment initiations;
2. Cancellation of any future dated payments: single, bulk or recurring;
3. Update the recurring payment parameters.

7. Glossary of Terms

Acronym	Term	Definition	Example
AIS	Account Information Services	Refers to the services (API's) offered by the ASPSP to retrieve account information. This can be balances, transactions or details about name, limits etc.	
AISP	Account Information Service Provider	Any financial provider that wishes to aggregate online account information of one or more accounts held at one or multiple ASPSPs (banks). This service can be used in accounting or generation of dashboards for a single	

Acronym	Term	Definition	Example
		customer.	
API	Application Programming Interface	In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software. A good API makes it easier to develop a computer program by providing all the building blocks, which are then put together by the programmer. An API may be for a web-based system, operating system, database system, computer hardware, or software library. An API specification can take many forms, but often includes specifications for routines, data structures, object classes, variables, or remote calls. POSIX, Microsoft Windows API, the C++ Standard Template Library, and Java APIs are examples of different forms of APIs. Documentation for the API is usually provided to facilitate usage. The status of APIs in intellectual property law is controversial.	
ASPSP	Account Servicing Payment Service Providers	Provides and maintains (current, savings, card) accounts, traditionally the core business of a bank.	HSBC, UniCredit
EBA	The European Banking Authority	An independent EU authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector.	
NextGenPSD2	NextGenPSD2 Access to	About The 'Berlin Group' is a pan-European payments	

Acronym	Term	Definition	Example
	Account Framework as defined by the Berlin Group	interoperability standards and harmonisation initiative with the primary objective of defining open and common scheme- and processor-independent standards in the interbanking domain between Creditor Bank (Acquirer) and Debtor Bank (Issuer), complementing the work carried out by e.g. the European Payments Council. As such, the Berlin Group has been established as a pure technical standardisation body, focusing on detailed technical and organisational requirements to achieve this primary objective.	
OAuth	Open (standard) authorization	OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. OAuth is used by several steps in the processes between the TPU and the ASPSP for things like Granting the TPP to access Account Information.	
PIS	Payment Initiation Services	Refers to the services (API's) offered by the ASPSP to initiate a new transaction (payment instruction). Most likely these services also have endpoints for authorisation and status updates.	
PISP	Payment Initiation Service Provider	Any organization (like a retailer) that can initiate credit transfers on behalf of the client.	Amazon
PSD	Payments Systems Directive	The Directive on Payment Services (PSD) provides the legal foundation for the creation of an EU-wide single market for payments. The PSD aims to establish a modern and comprehensive set of rules	

Acronym	Term	Definition	Example
		applicable to all payment services in the European Union. The goal is to make cross-border payments as easy, efficient and secure as national payments within a Member State.	
PSD1	Payments Systems Directive 1	Provides the necessary legal platform for the Single Euro Payments Area (SEPA).	
PSD2	Payments Systems Directive 2	Provides the necessary legal platform and changes to the payments framework in order to better serve the needs of an effective European payments market, fully contributing to a payments environment which nurtures competition, innovation and security to the benefits of all stakeholders and consumers in particular.	
PSU	Payment Service User	The end-user (the real customer) of PSD2 services.	
RTS	Regulatory Technical Standards	A detailed set of compliance standards (currently still under discussion) to be met by all parties. Standards cover data security, compensation, accountability, etc.	
SCA	Strong Customer Authentication	Defined by the EBA in its RTS on SCA as an authentication based on the use of two or more elements categorised as knowledge (something only the user knows [for example, a password]), possession (something only the user possesses [for example, a particular cell phone and number]) and inherence (something the user is [or has, for example, a fingerprint or iris pattern]) that are independent, [so] the breach of one does not compromise the others, and is designed in such a way as to	

Acronym	Term	Definition	Example
		protect the confidentiality of the authentication data.	
TPP	Third Party Provider	Third party provider is the collective name for AISPs and PISPs.	
XS2A	Access to Accounts	Access to Accounts enables financial institutions (like banks) and non-financial organizations to obtain access to the bank accounts of European consumers.	