iCard Open banking API

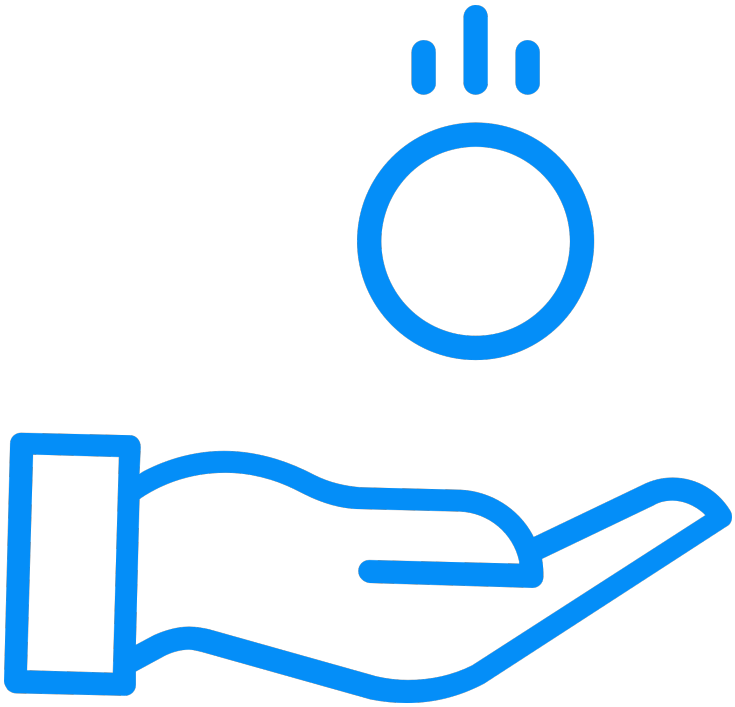
iCard Open Banking API

Definition

The Payment Services Directive (PSD, Directive 2007/64/EC, replaced by PSD2, Directive (EU) 2015/2366) is an EU Directive, administered by the European Commission (Directorate General Internal Market) to regulate payment services and payment service providers throughout the European Union (EU) and European Economic Area (EEA). The Directive's purpose was to increase pan-European competition and participation in the payments industry also from non-banks, and to provide for a level playing field by harmonizing consumer protection and the rights and obligations for payment providers and users.

AISP Services

Account information services



PISP Services

Payment initiation services

COF Services

Confirmation of funds service

Transport layer

TLS 1.2 or higher is mandatory. The TLS connection has to be established always including client (TPP) authentication. For this authentication the TPP has to use a qualified certificate for website authentication. This qualified certificate has to be issued by a qualified trust service provider according to the eIDAS regulation. The content of the certificate has to be compliant with the requirements of EBA-RTS. The certificate of the TPP has to include all roles the TPP is authorised to use..

API Structure

The interface is resource orientated. Resources can be addressed under the API endpoints Base URI – https://{provider}/v1/{service}{?query-parameters} using additional content parameters {parameters} where:

- {provider} is the host and path of the XS2A API, which is not further mentioned.

The host or path may contain release version information of the ASPSP.

- v1 is denoting the final version 1.3 of the Berlin Group XS2A interface Implementation Guidelines.
- {service} has the values
    - consents
    - payments
    - accounts
    - card-accounts
    - funds-confirmation
- {?query-parameters} are parameters detailing GET based access methods
- parameters} are content attributed defined in JSON

The structure of the request/response is described according to the following categories

- Path: Attributes encoded in the Path, e.g. “payment/sepa-credit-transfers” for {resource}
- Query Parameters: Attributes added to the path after the ? sign as process steering flags or filtering attributes for GET access methods. Query parameters of type Boolean shall always be used in a form query-parameter=true or query-parameter=false
- Header: Attributes encoded in the HTTP header of request or response
- Request: Attributes within the content parameter set of the request

Response: Attributes within the content parameter set of the response, defined in JSON

Account information services

iCard uses the oAuth2 standard for SCA to provide TPP access to the PSU account information.

Steps

1.Request Account Information

- The PSU consents to allow an AISP to access account information data.

2.Setup Account Access Consent

- The AISP connects to iCard PSD2 API and creates a consent resource. This informs iCard that one of the PSUs is granting access to account and maybe balance and transaction information to an AISP. iCard responds with an identifier of the created resource (the consentId). This step is carried out by making an HTTP POST request to /consents endpoint.
- The consent resource will include the permissions and optionally an expiration date after which, the AISP will no longer have access to the PSU’s data.

3.Authorise Consent

- The AISP requests the PSU to authorise the consent.
- The PSU is redirected to iCard to authorise the consent
- After and approval or decline of the requests, the PSU is redirected back to the AISP.
- During authorisation, the PSU selects accounts that are authorised for the AISP request in ASPSP (iCard) web account interface.

4.Request Data

- This is carried out by making a GET request to the relevant resource
- The unique account ids that are valid for the specific consent will be returned with a call to GET /accounts. This should always be the first call once the AISP has a valid access token from the consent.

Payment initiation services

Based on the PSU, iCard supports initiation and confirmation of cross border and SEPA payments and BISERA (Bulgarian domestic) Payments

Step

1.Request Payment Initiation

- This flow begins with the PCU consenting to a payment being made. The request is sent through a PISP.
- The debtor account details can optionally be specified at this stage.

2.Setup Payment Initiation

- The PISP connects to ASPSP (iCard) that services the PSU’s payment account and creates a new payment resource. This informs the ASPSP that one of its PSUs intends to make a payment. The APSPS responds with an identifier for the resource (paymentId).
- This step is carried out by making a POST request to the payments resource.

3.Authorise Payment

- The PISP redirects the PSU to the ASPSP. The redirect includes the paymentId generated in the previous step. This allows the ASPSP to correlate the payment that was setup. The ASPSP authenticates the PSU. The ASPSP updates the state of the payment resource internally to indicate the payment has been authorized.
- The PSU selects the debtor account at this stage in case it has not been previously specified in Step 1.
- The PSU is redirected back to the PISP.

4.Get Payment Status

- The ASPSP provides a status API, the PISP can check the status of the payment by passing the paymentId.

Become partner

- Register on our developers portal.
- Create an application.
- Use the application's Key and Secret to generate an oAuth token with grant type "client_credentials" using our Auth API.
- Use the token to create a consent request.
- Redirect your client to the link in the response to authenticate to consent.
- After confirmation, the client will be redirected back to the specified "redirect_uri" of the application with a GET parameter "code"
- Use the returned "code" parameter to generate an oAuth token with grant type "authorization_code".
- Use the returned oAuth token to access AIS, PIS and COF functionalities of the API.