

# Banca Mediolanum NextGenPSD2 XS2A Framework Implementation

Version 1.0.3

## Index

1	Aim of the document.....	3
2	References .....	3
3	Document History .....	4
4	Introduction.....	5
5	Secure connection.....	8
6	Third Party Validation .....	9
7	Usage of OAuth2 for PSU Authentication and Authorisation.....	10
7.1	Obtaining OAuth 2.0 access tokens .....	10
8	Redirect SCA Approach with Implicit Start of the Authorisation Process .....	15
9	Payment Initiation Service .....	16
9.1	Payment Initiation with JSON encoding of the Payment Instruction.....	16
9.2	Get Transaction Status Request .....	21
9.3	Get Payment Request.....	23
10	Account Information Service .....	26
10.1	Consent Request on Dedicated Accounts .....	26
10.2	Get Status Request .....	30
10.3	Get Consent Request.....	31
10.4	Delete an Account Information Consent Object.....	34
10.5	Read Account List .....	35
10.6	Read Account Details .....	37
10.7	Read Balance.....	39
10.8	Read Transactions .....	41
11	Confirmation of Funds Service.....	46
11.1	Confirmation of Funds Request.....	46

## 1 Aim of the document

This document aims to detail Banca Mediolanum's implementation of the NextGenPSD2 XS2A Framework from a technical point of view.

## 2 References

The following document refers to the Implementation Guidelines produced by the Berlin Group.

For all parts not specified in this document, please refer to the following original documents:

- BGV1.3: NextGenPSD2 Access to Account Interoperability Framework - Implementation Guidelines V1.3\_20181019.pdf  
<https://www.berlin-group.org/nextgenpsd2-downloads>

## 3 Document History

Version	Change/Note	Date
1.0	First version	13/03/2019
1.0.1	Added element payment-product in Payment Initiation Service endpoints.	14/03/2019
1.0.2	Added clarifications about time limits of authorization code and SCA redirect url.	18/03/2019
1.0.3	Modified access attribute description of Consent Request.	05/04/2019

## 4 Introduction

Banca Mediolanum exposes PSD2 APIs for Payment Initiation Service Provider (PISP) TPP, Account Information Service Provider (AISP) TPP and Payment Instrument Issuing Service Provider (PIISP) TPP in two different URLs:

- <https://api.mediolanum.it>
- <https://sandbox.mediolanum.it>

The first URL is for all APIs of *live* environment where services work on real and actual data of users; the second URL is for all APIs of *sandbox* environment that replicates main functionalities of the production environment but is completely isolated from it.

Banca Mediolanum provides a *sandbox* environment that allows TPP developers to validate their code before migrating it to the *live* environment.

For this reason, resources of Banca Mediolanum's XS2A Interface can be addressed under the following API endpoints:

- <https://api.mediolanum.it/psd2bg/{national bank code}/v1/{service}{?query-parameters}>
- <https://sandbox.mediolanum.it/psd2bg/{national bank code}/v1/{service}{?query-parameters}>

using additional content parameters {parameters}

where

- {national bank code} is the identifier of the ASPSP as reported in the list above
- v1 is denoting the final version 1.3 of the Berlin Group XS2A interface implementation Guidelines
- {service} has the values consents, payments, accounts or funds-confirmation, eventually extended by more information on product types and request scope
- {?query-parameters} are parameters detailing GET based access methods, e.g. for filtering content data
- {parameters} are content attributes defined in JSON encoding

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

- Path: attributes encoded in the path
- Query Parameters: attributes added to the path after the ? sign as process steering flags or filtering attributes for GET access methods
- 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

The following tables gives an overview on the HTTP access methods supported by the API endpoints and by resources created through this API:

Endpoints/Resources	Method
payments/{payment-product}	POST
payments/{payment-product}/{paymentId}	GET
payments/{payment-product}/{paymentId}/status	GET
accounts	GET
accounts/{accountId}	GET
accounts/{accountId}/balances	GET
accounts/{accountId}/transactions	GET
consents	POST
consents/{consentId}	GET
consents/{consentId}	DELETE
consents/{consentId}/status	GET
funds-confirmations	POST

The following table shows the possible HTTP response codes:

Status Code	Description
200 OK	<p>PUT, GET Response Codes</p> <p>This return code is permitted if a request was repeated due to a time-out.</p> <p>The POST for a Funds request will also return 200 since it does not create a new resource.</p>
201 Created	POST response code where Payment Initiation or Consent Request was correctly performed.
204 No Content	DELETE response code where a consent resource was successfully deleted. The code indicates that the request was performed, but no content was returned.
400 Bad Request	Validation error occurred. This code will cover malformed syntax in request or incorrect data in payload.
401 Unauthorized	The TPP or the PSU is not correctly authorized to perform the request. Retry the request with correct authentication information.
404 Not found	Returned if the resource or endpoint that was referenced in the path does not exist or cannot be referenced by the TPP or the PSU.
405 Method Not Allowed	This code is only sent when the HTTP method (PUT, POST, DELETE, GET etc.) is not supported on a specific endpoint.

408 Request Timeout	The server is still working correctly, but an individual request has timed out.
429 Too Many Requests	The TPP has exceeded the number of requests allowed by the consent or by the RTS.
500 Internal Server Error	Internal server error occurred.
503 Service Unavailable	The server is currently unavailable. Generally, this is a temporary state.

Additional error information are transmitted following NextGenPSD2 XS2A specification, as reported in the JSON example below:

```
{
  "tppMessages": [
    {
      "category": "ERROR",
      "code": "TOKEN_INVALID",
      "text": "additional text information of the ASPSP up to 512 characters"
    }
  ]
}
```

## 5 Secure connection

The communication between the TPP and the Banca Mediolanum NextGenPSD2 XS2A is always secured via a TLS-connection using TLS version 1.2 or higher. The TPP has to set-up this TLS-connection, authenticating itself (client authentication) through the use of a qualified certificate for website authentication (QWAC). 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 on SCA and SCS, Article 34. The certificate of the TPP has to indicate all roles the TPP is authorized for.

In this first stage, exclusively for the sandbox environment, Banca Mediolanum has decided to offer to Third Party Provider an additional registration process within Banca Mediolanum portal: through this process, an interested TPP that did not get an eIDAS certification or the NCA Authorization (or both) could access the Banca Mediolanum NextGenPSD2 XS2A for testing purposes.



## 6 Third Party Validation

Banca Mediolanum's NextGenPSD2 XS2A has to validate TPP identity and authorization status.

For identity validation, Banca Mediolanum's NextGenPSD2 XS2A relies on eIDAS certificate information that are verified through the inquiry on the Certificate Status Service provided by the QTSP who released the certification for the TPP (through CRL or OCSP). N.B. this step is discarded in case of a TPP registered within the portal in sandbox environment.

For authorization validation, Banca Mediolanum's NextGenPSD2 XS2A has to verify online if the authorization reported in the Certificate is still valid, through an online inquiry on NCA register (or equivalent source). N.B. this step is discarded in case of a TPP registered within the portal in sandbox environment.

## 7 Usage of OAuth2 for PSU Authentication and Authorisation

Banca Mediolanum implements OAuth2 as a support for the authorisation of the PSU towards the TPP for the payment initiation and/or account information service. In this case, the TPP is the client, the PSU the resource owner and the ASPSP is the resource server in the abstract OAuth2 model.

In particular, Banca Mediolanum supports it as an authentication of a PSU in a pre-step, translating this authentication into an access token to be used at the XS2A interface afterwards. By using OAuth2, the XS2A API calls work with an access token instead of using the PSU credentials.

### 7.1 Obtaining OAuth 2.0 access tokens

The following steps show how TPP's application interacts with Banca Mediolanum 's OAuth 2.0 server to obtain a PSU's consent to perform an API request on the PSU's behalf. TPP's application must have that consent before it can execute a call to NextGenPSD2 XS2A API that requires PSU authorization.

The list below quickly summarizes these steps:

1. TPP's application identifies the permissions it needs.
2. TPP's application redirects the PSU to ASPSP along with the requested permission.
3. PSU decides whether to grant the permission to TPP's application.
4. TPP's application finds out what the PSU decided.
5. If the PSU grants the requested permissions, TPP's application retrieves tokens needed to make API requests on the PSU's behalf.

#### Step 1: Set authorization parameters

TPP's first step is to create the authorization request. That request sets parameters that identify the application and define the permissions that the PSU will be asked to grant to TPP's application.

In order to obtain Banca Mediolanum 's OAuth 2.0 endpoint, TPP has to call one the NextGenPSD2 XS2A APIs without a valid access token. In this case, Banca Mediolanum will return an HTTP 401 Unauthorized response similar to the following:

```
{
  "status": 401,
  "status_message": "Unauthorized",
  "url": "{endpoint}"
}
```

```
}

```

The url attribute will contain an endpoint accessible only over HTTPS. Plain HTTP connections are refused.

TPP has to redirect PSU's web browser to this endpoint, adding the following query string parameters:

Parameter	Description
client_id	Required. The client ID for TPP's application. TPP can find this value in the API Portal, one for each available application (PIS, AIS).
redirect_uri	Required. Determines where the API server redirects the PSU after the PSU completes the authorization flow. The value must exactly match the authorized redirect URI for the OAuth 2.0 client, which TPP configured in the API Portal.
scope	Required. One of the scopes that identify the resources that TPP's application could access on the PSU's behalf. Acceptable scopes are: <ul style="list-style-type: none"> <li>"pisp.pagamento": to access Payment Initiation Service</li> <li>"aisp.base": to access Account Information Service</li> </ul>
state	Recommended. Specifies any string value that TPP's application uses to maintain state between its authorization request and the authorization server's response. The server returns the exact value that TPP sends as a name=value pair in the hash (#) fragment of the redirect_uri after the PSU consents to or denies application's access request.  TPPs can use this parameter for several purposes, such as directing the PSU to the correct resource in their application, sending nonces, and mitigating cross-site request forgery. Since the redirect_uri can be guessed, using a state value can increase the assurance that an incoming connection is the result of an authentication request. If TPPs generate a

	random string or encode the hash of a cookie or another value that captures the client's state, they can validate the response to additionally ensure that the request and response originated in the same browser, providing protection against attacks such as cross-site request forgery.
--	--

## Step 2: Redirect to Banca Mediolanum's OAuth 2.0 server

TPP redirects the PSU to Banca Mediolanum's OAuth 2.0 server to initiate the authentication and authorization process.

## Step 3: Banca Mediolanum prompts user for consent

In this step, PSU decides whether to grant TPP's application the requested access. At this stage, Banca Mediolanum 's OAuth 2.0 server authenticates the PSU and obtains consent from the PSU for TPP's application to access the requested scope.

TPP's application doesn't need to do anything at this stage as it waits for the response from Banca Mediolanum 's OAuth 2.0 server indicating whether the access was granted. That response is explained in the following step.

## Step 4: Handle the OAuth 2.0 server response

The OAuth 2.0 server responds to TPP's application's access request by using the URL specified in the request.

If PSU approves the access request, then the response contains an authorization code. If PSU does not approve the request, the response contains an error message. The authorization code that is returned to the web server appears on the query string, as shown below:

```
{redirect_uri}?code=4/P7q7W91a-oMsCeLvIaQm6bTrgtp7&state={state}
```

where:

redirect\_uri and state are the query string parameters set by TPP and above described.

If PSU denies the access request, the API server redirect the PSU to the cancel redirect URI which TPP configured in the API Portal.

## Step 5: Exchange authorization code for refresh and access tokens

After TPP receives the authorization code, it can exchange the authorization code for an access token within 30 seconds, after which the authorization code expires.

To exchange an authorization code for an access token, TPP has to call the specific endpoint

- <https://api.mediolanum.it:9090/oauth/token>

- <https://sandbox.mediolanum.it:9091/oauth/token>

and set the following parameters:

Parameter	Description
code	The authorization code returned from the initial request.
client_id	The client ID obtained from the API Portal.
client_secret	The client secret obtained from the API Portal (required only if TPP has chosen to be identified as "confidential" in the API Portal).
redirect_uri	The redirect URI listed in the API Portal.
grant_type	As defined in the OAuth 2.0 specification, this field must contain a value of <code>authorization_code</code> .

The following snippet shows a sample request:

```
POST /oauth/token HTTP/1.1

code=4/P7q7W91a-oMsCeLvIaQm6bTrgtp7&
client_id={tpp_client_id}&
client_secret={tpp_client_secret}&
redirect_uri={redirect_uri}&
grant_type=authorization_code
```

Banca Mediolanum responds to this request by returning a JSON object that contains an access token.

The response contains the following fields:

Parameter	Description
access_token	The token that TPP's application sends to authorize a request.
expires_in	The remaining lifetime of the access token in seconds.
token_type	The type of token returned. At this time, this field's value is always set to Bearer.

The following snippet shows a sample response:

```
{
  "access_token": "1/ffAGRNJru1FTz70BzhT3Zg",
  "expires_in": 3920,
```

```
"token_type": "Bearer"  
}
```

## 8 Redirect SCA Approach with Implicit Start of the Authorisation Process

The supported flow for Payment Initiation Service and Account Information Service, is the Redirect SCA Approach with Implicit Start of the Authorisation Process.

Within this flow, Account Information Consent and Payment Initiation Requests are followed by a redirection to the ASPSP SCA authorisation site.

The URL of the ASPSP SCA authorisation site are contained in the "scaRedirect" attribute of "\_links" attribute of responses of both calls.

TPP has to redirect PSU's web browser to the URL and wait for PSU SCA authentication. Note that, exclusively for Payment Initiation Service, ASPSP SCA site prevents the authorization from PSU if more than 60 seconds passed between the start of the flow and the redirection to the URL.

Once PSU has authorised or rejected, TPP will receive a redirect on one of the URI defined in the TPP-Redirect-URI and TPP-Nok-Redirect-URI headers of the request.

## 9 Payment Initiation Service

The Payment Initiation Flow that Banca Mediolanum has adopted is the Redirect SCA Approach with Implicit Start of the Authorisation Process. With this flow, the Account Information Consent Request is followed by a redirection to the ASPSP SCA authorization site.

### 9.1 Payment Initiation with JSON encoding of the Payment Instruction

POST /v1/payments/{payment-product}

This creates a payment initiation request at the ASPSP.

#### Path Parameters

Attribute	Type	Description
payment-product	String	The addressed payment product endpoint, e.g. for SEPA Credit Transfers (SCT). The list of products supported by Banca Mediolanum is: sepa-credit-transfers target-2-payments cross-border-credit-transfers

#### Query Parameters

No specific query parameters defined.

#### Request Header

Attribute	Type	Condition	Description
Content-Type	String	Mandatory	application/json
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Mandatory	Bearer Token.



PSU-IP-Address	String	Mandatory	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP.  If not available, the TPP shall use the IP Address used by the TPP when submitting this request.
TPP-Redirect-URI	String	Mandatory	URI of the TPP, where the transaction flow shall be redirected to after a Redirect.
TPP-Nok-Redirect-URI	String	Optional	If this URI is contained, the TPP is asking to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the redirect SCA method.

### Request Body

Currently, the only type of payment supported is "single payment".

The following table gives an overview on the JSON structures of standard SEPA payment products for single payments:

Data Element	Type	SCT EU Core	Target2 Paym. Core	Cross Border CT Core
debtorAccount (incl. type)	Account Reference	mandatory	mandatory	mandatory
instructedAmount (inc. Curr.)	Amount	mandatory	mandatory	mandatory
creditorAccount	Account Reference	mandatory	mandatory	mandatory
creditorName	Max70Text	mandatory	mandatory	mandatory

creditorAgent	BICFI	optional	optional	mandatory
creditorAddress	Address	optional	optional	mandatory
remittance Information Unstructured	Max140Text	mandatory	mandatory	mandatory

## Response Code

The HTTP response code equals 201.

## Response Header

Attribute	Type	Condition	Description
Location	String	Mandatory	Location of the created resource (if created)
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-SCA-Approach	String	Mandatory	REDIRECT

## Response Body

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	Possible values are: ACTC, CANC, RJCT, ACSC
paymentId	String	Mandatory	Resource identification of the generated payment initiation resource.
transactionFees	Amount	Mandatory	It can be used by the ASPSP to transport transaction fees relevant for the

			underlying payments.
_links	Links	Mandatory	<p>A list of hyperlinks to be recognised by the TPP.</p> <p>"scaRedirect": The link to which to redirect the PSU browser according to the SCA Redirect Approach.</p> <p>"self": The link to the payment initiation resource created by this request. This link can be used to retrieve the resource data.</p> <p>"status": The link to retrieve the transaction status of the payment initiation.</p>

### Example

Request
<pre> POST https://api.mediolanum.it/psd2bg/03062/v1/payments/cross-border-credit-transfers X-Request-ID: request-0001 PSU-IP-Address: 91.198.174.192 Content-Type: application/json Authorization: Bearer 1diS526vZhi74oUZw2iJ6td4p5zR39mZ94tAy1vYqmF0KmtX16S0pJ {   "debtorAccount": {     "iban": "IT42Z0306200120000000862916"   },   "instructedAmount": { </pre>

```
"currency": "EUR",
"amount": "1.00"
},
"creditorAccount": {
  "iban": "IT23J0306204010000001063502"
},
"creditorName": "name",
"creditorAgent": "agent",
"creditorAddress": {
  "city": "city",
  "country": "country"
},
"remittanceInformationUnstructured": "description"
}
```

## Response

```
{
  "transactionStatus": "ACTC",
  "paymentId": "Id-f718885c2c5e13b83dd689f4",
  "otp": "656a7960-b05b-499f-977c-62939fef92cc",
  "transactionFees": {
    "currency": "EUR",
    "amount": "5.160"
  },
  "_links": {
    "scaRedirect": {
      "href": "
https://api.mediolanum.it:9090/payment/confirm?abi=03062&lang=IT&d
=eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiaWwiYWxnIjoiaU1NBLU9BRVAzMjU2In0.cXJ3F
K8eiYEyIhqD-
af54hYFb5jKkTR45eUgIITIdvFRjxan6fgY__uQX5vI4QxhqwDK2fBkbTy1npLRxYS
9KTtDEA5we-
XJhTs4Zs08QAZ6rC_J9AJ7597kTeH21TtLyw1u4KRPg6R8RzgBByrD3WhpiDvL4T5R
nc1_nByncHi1AUuqGm1c9U1dbCUG61fGly74EpxIc2mP1NvvUKMk9w1Jf6HZFJQWmA
eMz2wptoFr6M_stpQflvHCu41bx7kB-
kQTLtyf0ssuDaTNZBnvxHpb3_kVgY6UGEDPj1mZbRLaaLTkK0YM-
Fm1voaj4wHm43xo03rLJxAS1t85vLtMkg.GdXxHtITShODHnGgXUtq9A.Yc-
TVVclmg73jxQsmK637UuzrA9UI_6SEiL8zHHI9-_W05aqHks0-
d1JPQBoHAlIUCF47aViGGGxip8IKSwuFkn7DwKw5-
7fsXZYAeDkPhdBJYiJ71suv3yunX2CZysOdPursNT4DoJSJtZdzENzSdgMi0VxOPT8
Q_DgDi68L6d14Ekhsj066z9xh0ILLo0QymEJK0bFF8hh6pFsdTtv1BR3kqdS0JcPD
dGyuRLgemHT9HcABp1J8AqheXEdoS-
```

```
b2X5owFoWdFwxFA40vBE0vVz0dfJ1ztYhhJBFX2V8W4f6si9nXg_zbQfH0m1ARoiOp
86EciBx2EUw3kXDKIIPLGEx0ZnXLEBhRo9b_xkmhSRoVjMtDJfr_WeqVhNxALGL2V2
NhCG_5v3Yt0Fv0bPHQ.yUEk5B0uK4VxV7aGdc1VPg"
    }
  }
}
```

## 9.2 Get Transaction Status Request

GET /v1/{payment-service}/{payment-product}/{paymentId}/status

Can check the status of a payment initiation.

### Path Parameters

Attribute	Type	Description
payment- product	String	The addressed payment product endpoint, e.g. for SEPA Credit Transfers (SCT). The list of products supported by Cedacri is: sepa-credit-transfers target-2-payments cross-border-credit-transfers
payment-service	String	The only admitted value is: payments
paymentId	String	Resource Identification of the related payment.

### Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Mandatory	Bearer Token.
Accept	String	Optional	Only JSON format is supported.

### Query Parameters

No specific query parameters defined.

## Request Body

No request body.

## Response Code

The HTTP response code equals 200.

## Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

## Response Body

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	Possible values are: ACTC, CANC, RJCT, ACSC

## Example

Request
<pre>GET https://api.mediolanum.it/psd2bg/03062/v1/payments/sepa-credit-transfers/Id-87e3885cdd761b0c38f6af2d/status X-Request-ID: request-0001 Authorization: Bearer 1diS526vZhi74oUZw2iJ6td4p5zR39mZ94tAy1vYqmFOKmtX16S0pJ</pre>
Response
<pre>HTTP/1.1 200 X-Request-ID: request-0001 Content-Type: application/json {   "transactionStatus": "ACTC" }</pre>

## 9.3 Get Payment Request

GET /v1/{payments-service}/{payment-product}/{paymentId}

Returns the content of a payment object.

### Path Parameters

Attribute	Type	Description
payment- product	String	The addressed payment product endpoint, e.g. for SEPA Credit Transfers (SCT). The list of products supported by Cedacri is: sepa-credit-transfers target-2-payments cross-border-credit-transfers
payment-service	String	payments
paymentId	String	ID of the corresponding payment initiation object as returned by an Payment Initiation Request

### Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Mandatory	Bearer Token.

### Query Parameters

No specific query parameters defined.

### Request Body

No request body.

## Response Code

The HTTP response code equals 200.

## Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

## Response Body

The response body is dependent on the parameter {payment-service}. It contains the view of the ASPSP on the addressed payment resource.

Data Element	SCT EU Core	Target2 Paym. Core	Cross Border CT Core
debtorAccount (incl. type)	mandatory	mandatory	mandatory
instructedAmount (inc. Curr.)	mandatory	mandatory	mandatory
creditorAccount	mandatory	mandatory	mandatory
creditorName	mandatory	mandatory	mandatory
creditorAgent	optional	optional	mandatory
creditorAddress	optional	optional	mandatory
remittance Information Unstructured	optional	optional	optional
transactionStatus	mandatory	mandatory	mandatory
paymentId	mandatory	mandatory	mandatory
transactionFees	mandatory	mandatory	mandatory

## Example

Request
---------



```
GET https://api.mediolanum.it/psd2bg/03062/v1/payments/sepa-credit-transfers/Id-87e3885cdd761b0c38f6af2d
X-Request-ID: request-0001
Authorization: Bearer
ldiS526vZhi74oUZw2iJ6td4p5zR39mZ94tAy1vYqmFOKmtXl6SOpJ
```

### Response

```
HTTP/1.1 200
X-Request-ID: request-0001
Content-Type: application/json
{
  "debtorAccount": {
    "iban": "IT42Z0306200120000000862916"
  },
  "instructedAmount": {
    "currency": "EUR",
    "amount": "1"
  },
  "creditorAccount": {
    "iban": "IT23J0306204010000001063502"
  },
  "creditorName": "name",
  "remittanceInformationUnstructured": "description"
}
```

## 10 Account Information Service

The Account Information Consent Flow that Banca Mediolanum has adopted is the Redirect SCA Approach with Implicit Start of the Authorisation Process. With this flow, the Account Information Consent Request is followed by a redirection to the ASPSP SCA authorization site.

### 10.1 Consent Request on Dedicated Accounts Call

POST /v1/consents

Creates an account information consent resource at the ASPSP regarding access to accounts specified in this request.

#### Path Parameters

No specific path parameters defined.

#### Query Parameters

No specific query parameters defined.

#### Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Mandatory	Bearer Token.
TPP-Redirect-URI	String	Mandatory	URI of the TPP, where the transaction flow shall be redirected to after a Redirect.
TPP-Nok-Redirect-URI	String	Optional	If this URI is contained, the TPP is asking to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the redirect SCA method.

### Request Body

Attribute	Type	Condition	Description
access	Account Access	Mandatory	Supported values are: ... { "availableAccounts": "allAccounts" } ...
recurringIndicator	Boolean	Mandatory	true, if the consent is for recurring access to the account data  false, if the consent is for one access to the account data.
validUntil	ISODate	Mandatory	This parameter is requesting a valid until date for the requested consent. The content is the local ASPSP date in ISODate Format, e.g. 2017-10-30. If a maximal available date is requested, a date in far future is to be used: "9999-12-31". The consent object to be retrieved by the GET Consent Request will contain the adjusted date.
frequencyPerDay	Integer	Mandatory	This field indicates the requested maximum frequency for an access per day. For a one-off access, this attribute is set to "1".
combinedService Indicator	Boolean	Mandatory	false

## Response Code

The HTTP response code equals 201.

## Response Header

Attribute	Type	Condition	Description
Location	String	Mandatory	Location of the created resource.
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-SCA-Approach	String	Mandatory	REDIRECT

## Response Body

Attribute	Type	Condition	Description
consentStatus	Consent Status	Mandatory	authentication status of the consent
consentId	String	Mandatory	Identification of the consent resource as it is used in the API structure
_links	Links	Mandatory	<p>A list of hyperlinks to be recognised by the TPP.</p> <p>Type of links admitted in this response (which might be extended by single ASPSPs as indicated in its XS2A documentation):</p> <p>"scaRedirect": In case of an SCA</p>

			Redirect Approach, the ASPSP is transmitting the link to which to redirect the PSU browser.
--	--	--	---

## Example

Request
<pre>POST https://api.mediolanum.it/psd2bg/03062/v1/consents X-Request-ID: request-0001 TPP-Redirect-URI: https://tpp-redirect-ok-url Content-Type: application/json TPP-Nok-Redirect-URI: https://tpp-redirect-nok-url Authorization: Bearer o9xcq8V2zUg893gm6ROp07XDUhaBkIOyilSHGOM11XCXFgjMPP7U6R {   "access": {     "availableAccounts": "allAccounts"   },   "recurringIndicator": false,   "validUntil": "2019-10-10",   "frequencyPerDay": 1,   "combinedServiceIndicator": false }</pre>
Response
<pre>HTTP/1.1 201 ASPSP-SCA-Approach: REDIRECT X-Request-ID: request-0001 Content-Type: application/json {   "consentStatus": "received",   "consentId": "8c929c62-53f3-4543-97c0-0aed02b1d9bc",   "_links": {     "scaRedirect": {       "href": "https://api.mediolanum.it:9090/consent/init?consent_id=8c929c62-53f3-4543-97c0-0aed02b1d9bc&amp;d=eyJlbnMiOiJBMTI4Q0JDLUhTMjU2IiwiaWwiYWxnIjoiaU1NBLU9BRVAtMjU2In0.A5WAZn0nw3g2t8yBD6k0_J9gwhhaOpJBVtm53TgWv4Goo1wkWoe4MWP1mzZeysle9sTiG3y3CbViuAqgpvH_pY-WKic2ZQgoTtJtgSexp3FN78FHrxuThrQDvzX8hC3Q2W4cJjL9n70rPwTycZaJI-</pre>

```
GsHwGIN8Bi95AsgQk01XMAgU2a-Z1b11xTMH1_VXewppjhw_-
Xe7jcn1V6cd3UHsfVj6oLXTM4FkhVItd073ueFpdqWm8oTykrnCifhdt4mTGhgtSdB
qDjJlyDHMzt7EtheVPXbPFcw84Y-
ESXjSS1ubTZYxHNI87B0idEXXpZ0IKghtN0GG4h5sjtAEO_cw.ZRkTBQ1u2GoIaWxI
YiU-Bg.hKKNALi1_hWnCgXAsXoYGZrPpQaGw1bRPrQWMF9dXFJf_D08cz-
E3CejjqBZSkSDibT2kBFafZJkP0NaPxmQTtTc6aUTfERxMqX-
ImID57f0EZkiSoJz_n7ANg-
tkx7BP13eW5nTyNAYryVyYaEoELwRBeTeuUbOpADsWuZV4cXXOKsdSfde0cphMj7eu
WtmaYFuthEzELuXaOGZDqqKu3ENhVotbzdH0n_vKUs35Y.BH1s0M-
oxoStLffTPUb41Q"
    }
  }
}
```

## 10.2 Get Status Request

GET /v1/consents/{consentId}/status

Can check the status of an account information consent resource.

### Path Parameters

Attribute	Type	Description
consentId	String	The consent identification assigned to the created resource.

### Query Parameters

No specific query parameters defined.

### Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Mandatory	Bearer Token.

### Request Body

No request body.

## Response Code

The HTTP response code equals 200.

## Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

## Response Body

Attribute	Type	Condition	Description
consentStatus	Consent Status	Mandatory	This is the overall lifecycle status of the consent. Possible values are: received, valid, revokedByPsu, expired, terminatedByTpp.

## Example

Request
<pre>GET https://api.mediolanum.it/psd2bg/03062/v1/consents/8c929c62-53f3-4543-97c0-0aed02b1d9bc/status X-Request-ID: request-0001 Authorization: Bearer o9xcq8V2zUg893gm6R0p07XDUhaBkIOyilSHG0M11XCXFgjMPP7U6R</pre>
Response
<pre>HTTP/1.1 200 X-Request-ID: request-0001 Content-Type: application/json {   "consentStatus": "received" }</pre>

## 10.3 Get Consent Request

GET /v1/consents/{consentId}

Returns the content of an account information consent object. This is returning the data for the TPP especially in cases, where the consent was directly managed between ASPSP and PSU e.g. in a re-direct SCA Approach.

## Path Parameters

Attribute	Type	Description
consentId	String	ID of the corresponding consent object as returned by an Account Information Consent Request.

## Query Parameters

No specific query parameters defined.

## Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Mandatory	Bearer Token.

## Request Body

No request body.

## Response Code

The HTTP response code equals 200.

## Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

## Response Body

Attribute	Type	Condition	Description
access	Account Access	Mandatory	



recurringIndicator	Boolean	Mandatory	
validUntil	ISODate	Mandatory	
frequencyPerDay	Integer	Mandatory	
lastActionDate	ISODate	Mandatory	This date is containing the date of the last action on the consent object either through the XS2A interface or the PSU/ASPSP interface having an impact on the status.
consentStatus	Consent Status	Mandatory	The status of the consent resource. Possible values are: received, valid, revokedByPsu, expired, terminatedByTpp.

### Example

Request
<pre>GET https://api.mediolanum.it/psd2bg/03062/v1/consents/8c929c62-53f3-4543-97c0-0aed02b1d9bc X-Request-ID: request-0001 Authorization: Bearer o9xcq8V2zUg893gm6R0p07XDUhaBkIOyilSHGOM11XCXFgjMPP7U6R</pre>
Response
<pre>HTTP/1.1 200 X-Request-ID: request-0001 Content-Type: application/json {   "access": {     "availableAccounts": "allAccounts"   },   "recurringIndicator": false,   "validUntil": "2019-10-10 00:00 AM UTC",   "frequencyPerDay": 1,   "lastActionDate": "2019-03-09 10:07 AM UTC",</pre>

```
"consentStatus": "received"
}
```

## 10.4 Delete an Account Information Consent Object

DELETE /v1/consents/{consentId}

Deletes a given consent (sets the status to terminatedByTpp).

### Path Parameters

Attribute	Type	Description
consentId	String	Contains the resource-ID of the consent to be deleted.

### Query Parameters

No specific query parameters defined.

### Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Mandatory	Bearer Token.

### Request Body

No request body.

### Response Code

The HTTP response code equals 204.

### Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call,

			as determined by the initiating party.
--	--	--	--

## Response Body

No response body.

## Example

Request
DELETE https://api.mediolanum.it/psd2bg/03062/v1/consents/8c929c62-53f3-4543-97c0-0aed02b1d9bc X-Request-ID: request-0001 Authorization: Bearer o9xcq8V2zUg893gm6R0p07XDUhaBkIOyilSHG0M11XCXFgjMPP7U6R
Response
HTTP/1.1 204 No Content X-Request-ID: request-0001

## 10.5 Read Account List

GET /v1/accounts

Reads a list of bank accounts.

### Path Parameters

No specific path parameters defined.

### Query Parameters

No specific query parameters defined.

### Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call,

			as determined by the initiating party.
Consent-ID	String	Mandatory	Shall be contained since "Establish Consent Transaction" was performed via this API before.
Authorization	String	Conditional	Bearer Token.

### Request Body

No request body.

### Response Code

The HTTP response code equals 200.

### Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

### Response Body

Attribute	Type	Condition	Description
accounts	Array of Account Details	Mandatory	

### Example

Request
<pre>GET https://api.mediolanum.it/psd2bg/03062/v1/accounts X-Request-ID: request-0001 Consent-ID: 8c929c62-53f3-4543-97c0-0aed02b1d9bc PSU-IP-Address: 91.198.174.192</pre>

```

Authorization: Bearer
o9xcq8V2zUg893gm6R0p07XDUhaBkIOyilSHGOM11XCXFgjMPP7U6R

```

---

**Response**

```

HTTP/1.1 200
X-Request-ID: request-0001
Content-Type: application/json
{
  "accounts": [
    {
      "iban": "IT42Z0306200120000000616474",
      "currency": "EUR"
    },
    {
      "iban": "IT42Z0306200120000000862916",
      "currency": "EUR"
    }
  ]
}

```

## 10.6 Read Account Details

GET /v1/accounts/{accountId}

Reads details about an account.

### Path Parameters

Attribute	Type	Description
accountId	String	This identification is denoting the addressed account. The accountId is retrieved by using a "Read Account List" call. The accountId is the "resourceId" attribute of the account structure. Its value is constant at least throughout the lifecycle of a given consent.

### Query Parameters

No specific query parameters defined.

### Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	Shall be contained since "Establish Consent Transaction" was performed via this API before.
Authorization	String	Conditional	Bearer Token.

## Request Body

No request body.

## Response Code

The HTTP response code equals 200.

## Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

## Response Body

Attribute	Type	Condition	Description
account	Account Details	Mandatory	

## Example

Request
<pre>GET https://api.mediolanum.it/psd2bg/03062/v1/accounts/IT42Z0306200120000000616474</pre>

<pre>X-Request-ID: request-0001 Consent-ID: 8c929c62-53f3-4543-97c0-0aed02b1d9bc PSU-IP-Address: 91.198.174.192 Authorization: Bearer o9xcq8V2zUg893gm6R0p07XDUhaBkIOyi1SHGOM11XCXFgjMPP7U6R</pre>
<b>Response</b>
<pre>HTTP/1.1 200 X-Request-ID: request-0001 Content-Type: application/json {   "iban": "IT42Z0306200120000000616474",   "currency": "EUR" }</pre>

## 10.7 Read Balance

GET /v1/accounts/{accountId}/balances

Reads account data from a given account addressed by "accountId".

### Path Parameters

Attribute	Type	Description
accountId	String	This identification is denoting the addressed account. The accountId is retrieved by using a "Read Account List" call. The accountId is the "resourceId" attribute of the account structure. Its value is constant at least throughout the lifecycle of a given consent.

### Query Parameters

No specific query parameters defined.

### Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call,

			as determined by the initiating party.
Consent-ID	String	Mandatory	Shall be contained since "Establish Consent Transaction" was performed via this API before.
Authorization	String	Conditional	Bearer Token.

### Request Body

No request body.

### Response Code

The HTTP response code equals 200.

### Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

### Response Body

Attribute	Type	Condition	Description
balances	Array of Balance	Mandatory	A list of balances regarding this account, e.g. the current balance, the last booked balance.

### Example

<b>Request</b>
----------------



GET https://api.mediolanum.it/psd2bg/03062/v1/accounts/IT42Z030620012000000616474/balances X-Request-ID: request-0001 Consent-ID: 8c929c62-53f3-4543-97c0-0aed02b1d9bc PSU-IP-Address: 91.198.174.192 Authorization: Bearer o9xcq8V2zUg893gm6ROp07XDUhaBkIOyilSHGOM11XCXFgjMPP7U6R
Response
HTTP/1.1 200 X-Request-ID: request-0001 Content-Type: application/json { "account": { "iban": "IT42Z0306200120000000616474" }, "balances": [ { "balanceAmount": { "currency": "EUR", "amount": "3" }, "balanceType": "expected", "referenceDate": "2019-02-23" }, { "balanceAmount": { "currency": "EUR", "amount": "3" }, "balanceType": "interimAvailable", "referenceDate": "2019-02-23" } ] }

## 10.8 Read Transactions

GET /v1/accounts/{accountId}/transactions {query-parameters}

Reads a list of transactions from a given account addressed by "accountId".

## Path Parameters

Attribute	Type	Description
accountId	String	This identification is denoting the addressed account. The accountId is retrieved by using a "Read Account List" call. The accountId is the "resourceId" attribute of the account structure. Its value is constant at least throughout the lifecycle of a given consent.

## Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	Shall be contained since "Establish Consent Transaction" was performed via this API before.
Authorization	String	Conditional	Bearer Token.
Accept	String	Optional	Only JSON format is supported.

## Query Parameters

Attribute	Type	Condition	Description
dateFrom	ISODate	Mandatory	Starting date (inclusive the date dateFrom) of the transaction list.
dateTo	ISODate	Optional	End date (inclusive the data dateTo) of the transaction list, default is "now" if not given.

bookingStatus	String	Mandatory	Permitted codes are: booked
---------------	--------	-----------	--------------------------------

## Request Body

No request body.

## Response Code

The HTTP response code equals 200.

## Response Header

Attribute	Type	Condition	Description
Content-Type	String	Mandatory	application/json
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

## Response Body

Attribute	Type	Condition	Description
transactions	Account Report	Mandatory	JSON based account report.

## Example

Request
<pre>GET https://api.mediolanum.it /psd2bg/03062/v1/accounts/IT42Z0306200120000000616474/transactions ?bookingStatus=booked&amp;dateFrom=2018-12-31&amp;dateTo=2019-01-01 X-Request-ID: request-0001 Consent-ID: 8c929c62-53f3-4543-97c0-0aed02b1d9bc Authorization: Bearer Ac85Cpl45c03tZiS5NcZ1cLAVCSLM8HUKL3HU2e6ddgFq494mCM5o8</pre>
Response
<pre>HTTP/1.1 200 X-Request-ID: request-0001</pre>

Content-Type: application/json

```
{
  "account": {
    "iban": "IT42Z0306200120000000616474"
  },
  "transactions": {
    "booked": [
      {
        "transactionAmount": {
          "currency": "EUR",
          "amount": "-2"
        },
        "bookingDate": "2019-02-19",
        "remittanceInformationUnstructured": "example"
      },
      {
        "transactionAmount": {
          "currency": "EUR",
          "amount": "-1"
        },
        "bookingDate": "2019-02-20",
        "remittanceInformationUnstructured": "example"
      },
      {
        "transactionAmount": {
          "currency": "EUR",
          "amount": "1"
        },
        "bookingDate": "2019-02-21",
        "remittanceInformationUnstructured": "example"
      },
      {
        "transactionAmount": {
          "currency": "EUR",
          "amount": "2"
        },
        "bookingDate": "2019-02-22",
        "remittanceInformationUnstructured": "example"
      },
      {
        "transactionAmount": {
```

```
        "currency": "EUR",  
        "amount": "3"  
    },  
    "bookingDate": "2019-02-23",  
    "remittanceInformationUnstructured": "example"  
  }  
  ]  
}  
}
```

## 11 Confirmation of Funds Service

### 11.1 Confirmation of Funds Request

POST /v1/funds-confirmations

Creates a confirmation of funds request at the ASPSP.

#### Path Parameters

No specific path parameters defined.

#### Query Parameters

No specific query parameters defined.

#### Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

#### Request Body

Attribute	Type	Condition	Description
account	Account Reference	Mandatory	PSU's account number.
instructedAmount	Amount	Mandatory	Transaction amount to be checked within the funds check mechanism.

#### Response Code

The HTTP response code equals 200.

#### Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call,

			as determined by the initiating party.
--	--	--	--

## Response Body

Attribute	Type	Condition	Description
fundsAvailable	Boolean	Mandatory	Equals true if sufficient funds are available at the time of the request, false otherwise.

## Example

Request
<pre>POST https://api.mediolanum.it/psd2bg/03062/v1/funds-confirmations X-Request-ID: request-0001 Content-Type: application/json {   "account": {     "iban": "IT42Z0306200120000000616474"   },   "instructedAmount": {     "currency": "EUR",     "amount": "1"   } }</pre>
Response
<pre>HTTP/1.1 200 X-Request-ID: request-0001 Content-Type: application/json {   "fundsAvailable": true }</pre>