Secure start and the new decoupled flow for BankID

External information

Document version 0.2

Change log

Version: 0.1

- First version

Version: 0.2

- English version

Reason for releasing a breaking change

During 2024, BankID will stop supporting today's solution where a static QR code is displayed. Animated QR codes will be used instead.

Differences between version 1.0 and 2.0 of the API

The main differences are as follows:

- When calling the initiation resource in the Authorization Server, the TPP (Third Party Provider) must submit if the PSU (Payment Service User) has a TPP client and BankID app (BISA) on the same device or on a different device.
- The response from the initiation resource will contain either a so called autoStartToken (on the same device) or a QR code (on a different device).
- The QR code has a short life span and must be re-generated as frequently as possible.
- When calling the "Decoupled Grant Token" resource, a new QR code will be returned as long as the PSU hasn't scanned any QR code.
- When calling the "Decoupled Grant Token" resource, the status value (i.e. the result) is returned and corresponds to the status values that BankID has for orders that are in progress but not completed.
- By stopping events and non-technical errors, the BankID order is cancelled and a HTTP status 400 is returned.
- The number of error codes returned with a HTTP status 400 has increased.The generic error code ”error”: ”mbid_error” has been replaced with different error codes.

MBID decoupled – version 2

This is a flow that requires several resource calls from TPPs to enable a PSU confirmation.
The Authorization server must establish an application state (i.e. session) during the flow.
The format of the request and response parameters, including error handling, are inspired by the Oauth2 protocol.

The resources involved are the following:

initAuthorization - Create an MBID order. Establish a "decoupled MBID session".
Token - Request to retrieve an access token. Can be invoked several times as long as the order is not completed or an error has occurred.
cancel - Cancel the ongoing order.

POST /initAuthorization/2.0

Initial resource to start a PSU confirmation with Mobile BankID.
The resource will invoke a BankID service to create a confirmation order in the BankID server.

A TPP must use an AutoStartToken or animated QR code to enable channel binding with the BankID app (BISA).

Request

URL: POST https://api.handelsbanken.com/mlurd/decoupled/mbid/initAuthorization/2.0
Headers:
Content-Type: application/json; charset=UTF-8
Accept: application/json
Body:

Name	Description
client_id	Mandatory. TPP identity. Format rules: 1-36 characters (0-9, a-z, A-Z, '_','-')
scope	Mandatory. A dynamic scope (a single scope combined with an intentId) The allowed format is: <scope> + ":" + <IntentId> A scope value is considered to be valid when it contains 1-36 characters (0-9, a –z, A-Z, '_', '-'). The intent id is considered to be valid when it contains 1-36 characters (0-9, a –z, A-Z, '_', '-').
psu_client_ip	Mandatory. PSU IP address. Both IPV4 and IPV6 address formats are allowed.
psu_id	Optional. PSU Personal Id. Swedish civic registration number, 12 digits.
bisa_same_device	Mandatory. Data type : boolean Set value to true when the customer BankID app (BISA) run on the same device as the TPP client. An autoStartToken will be returned in the response. Set value to false when the BISA app is run on a different device than the TPP client. A complete QR code will be returned in the response.

JSON Example – BISA and TPP client on the same device:

```
{
    "client_id" : “a3d59448-5439-49de-bffa-3e036242b001”,
    "scope" : “<scope>:<intentId>”,
    "psu_client_ip" : "192.102.28.2",
    "psu_id" : "190303033333”,
    "bisa_same_device" : true
}
```

JSON Example – BISA and TPP client on different devices:

```
{
    "client_id" : “a3d59448-5439-49de-bffa-3e036242b001”,
    "scope" : “<scope>:<intentId>”,
    "psu_client_ip" : "192.102.28.2",
    "psu_id" : "190303033333”,
    "bisa_same_device" : false
}
```

Response

Name	Description
auto_start_token	Optional. Will only be returned when bisa_same_device=true Token to use when auto starting BISA on the same device.
qr_code	Optional. Will only be returned when bisa_same_device=false A complete QR-code with a limited lifetime.
sleep_time	Mandatory. The minimum number of milliseconds to wait before invoking the token resource and between each call. Data type: Integer
_links	Mandatory. HAL links to the token and cancel resource.

JSON – When bisa_same_device=true (same as before):

```
{
    "auto_start_token" : "bca04b34-729d-4219-a540-d48391386b47",
    "sleep_time" : 1000,
    "_links" : {
        "token" : {
            "href" : "https://api.handelsbanken.com/mlurd/decoupled/mbid/token/2.0?sessionId=023",
            "hints" : { "allow" : [ "POST" ] }
        },
        "cancel" : {
            "href" : "https:// api.handelsbanken.com/mlurd/decoupled/mbid/cancel/2.0?sessionId=023",
            "hints" : { "allow" : [ "POST" ] }
        }
    }
}
```

JSON – When bisa_same_device=false:


```
{
    "qr_code" : "bankid.96a26d51-1378-48fa-be61-0035607a2eca.0.77024e4d….",
    "sleep_time" : 1000,
    "_links" : {
        "token" : {
            "href" : "https://api.handelsbanken.com/mlurd/decoupled/mbid/token/2.0?sessionId=023",
            "hints" : { "allow" : [ "POST" ] }
        },
        "cancel" : {
            "href" : "https:// api.handelsbanken.com/mlurd/decoupled/mbid/cancel/2.0?sessionId=023",
            "hints" : { "allow" : [ "POST" ] }
        }
    }
}
```


Error handling and validations

HTTP status 400, 500 or 503 can be returned.
Error handling is SHB specific but inspired by the Oauth2 specification. Status 500 “Internal Server Error” and 503 “Service Not Available” is returned with an empty body: {}.
The list below describes the error situations when the status 400 is returned.

Error	Description
invalid_request	Errors caused by the TPP. Missing required parameters, invalid parameters values.
Unauthorized_client	The TPP does not have the correct agreement to do a PSU confirmation for the scope or MBID decoupled is not allowed for the current consent.
intent_expired	Intent/consent has expired
mbid_already_started	A PSU has already started another BID order. Only one at a time is allowed. This attempt fails and the other will be cancelled by BankID.

POST /token/2.0

Create and return an access token when the MBID order has been confirmed by the PSU and BankID.

If the confirmation is ongoing, but not done, the HTTP status 200 is returned with a result parameter. The value in the result corresponds to a subset of the values documented by BankID in the “Relying Party Guidelines” document. Depending on the value, the TPP can act as specified in the guidelines.

The TPP can invoke the resource again after the time given in the initAuthorization reply.

If the BankID transaction and additional validations is successful, the HTTP status 200 is returned with a result saying “COMPLETE”. The response also includes the issued token.

If any event occurs which means that the order was not successful, including the user cancelling the transaction, the HTTP status 400 is returned. Different error codes that are found in the body, explain the reason why the transaction was terminated. When no additional calls to the resource can be done, a new initAuthorization call is required for a new attempt.

The resource will invoke a BankID service to ask for the status of the order.

The Authorization Server's maximum time for a Mobile BankID order to be completed in is 2 minutes.

In a scenario where the PSU uses two different devices, a QR code scanning is required before BISA tells BankID Server that a client exists. The QR code has a limited lifetime and each time the token-resource is invoked it will return a new QR code (as long as the PSU hasn't scanned it).
It is important that the TPP replaces the QR code as often as it can, but not more often than specified in the initAuthorization reply.

BankID will terminate the transaction if a scanning is not done within 30 seconds from the creation time of the transaction.

Request

URL: POST https://api.handelsbanken.com/mlurd/decoupled/mbid/token/2.0?sessionId=xyz
Headers:
Content-Type: application/json
Accept: application/json; charset=UTF-8
Body: { } empty JSON

Response

Name	Description
result	Status for the token. See BankID's "Relying Party Guidelines" for additional details. The following non completed result values can be returned by this resource: *outstandingTransaction* – When different devices, a new QR code is returned. *noClient* – When different devices, a new QR code is returned. *started* - When different devices, QR code has been scanned. No QR is returned. *userSign* – The transaction is in progress. No QR is returned. Regardless of which of above values that are returned, the TPP can invoke the resource again. *COMPLETE* - The PSU has verified and the response includes token info. No more invocations to the token resource can be done.
qr_code	A complete QR-code string with limited lifetime. Optional, will only be returned when the result is *outstandingTransaction* or *noClient* and bisa_same_device=false was used when calling the initAuthorization resource.
access_token	Token. Base64 encoded. Optional. Only returned when result=COMPLETE
token_type	Always the value "Bearer". Optional. Only returned when result=COMPLETE
expires_in	Number of seconds the access_token is valid for. Optional. Only returned when result=COMPLETE

refresh_token	Refresh token. Base64 encoded Optional. Only returned when result=COMPLETE and when the scope supports refresh.

JSON (outstandingTransaction or noClient and bisa_same_device=false):

```
{
    "result" : "< outstandingTransaction | noClient >",
   "qr_code" : "bankid.96a26d51-1378-48fa-be61-0035607a2eca.0.77025e5d…."
}
```

JSON (started or userSign):

```
{
    "result" : "< started | userSign >"
}
```

JSON (“COMPLETE”):

```
{
    "result" : "COMPLETE”,
    "access_token" : " QVQ6Y2Q4NmRkMTctMTA4",
    "token_type" : "Bearer",
    "expires_in" : 7776000,
    "refresh_token" : " VVV8Z2Q4NmRkMTdamad22"
}
```

Error handling and validations

HTTP status 400, 500 or 503 can be returned.

Error handling is SHB specific but inspired by the Oauth2 specification. Status 500 “Internal Server Error” and 503 “Service Not Available” is returned with an empty body: {}.

The list below describes the error situations when status 400 is returned.

error	**Description**
invalid_request	Errors caused by the TPP. Normally it will occur when a TPP invokes the resource after the transaction has been terminated, either because it was complete or an error occurred.
mbid_invalid_polling	TPP invokes the resource too often. Check that frequency is >= the time returned in the initAuthorization call (1 second).
mbid_transaction_expired	Maximum time has been reached (>2 minutes since order was created) . The order will be cancelled in BankID before the response is returned.
mbid_cancelled	BankID has cancelled the transaction, probably because the PSU started a new transaction.
mbid_user_cancelled	The PSU has cancelled the transaction in BISA.
mbid_start_failed	This is returned for a couple of reasons: - If the autostartToken was used and no BISA app is installed on the PSU’s device. - If the QR code was used and the QR code scanned was too old or the PSU didn’t scan it at all.
mbid_error	Other BankID related errors, i.e. error situations that are none of the above.
mbid_not_shb_activated	The PSU uses an external issued MBID that has not been confirmed by the PSU in either our mobile app or internet service during login.
not_shb_approved	The PSU does not have the correct agreement to confirm TPP usage.

POST /cancel/2.0

This is to cancel an ongoing verification. A TPP that provides the possibility for a PSU to cancel the verification in its user interface, can use this resource to cancel the transaction in the BankID environment.
If the PSU decides to confirm again, it may fail because the PSU already has an ongoing transaction. This situation will be prevented if the cancellation is implemented.

The resource must only be invoked for transactions that are still alive (an initAuthorization must have been successful and no previous error from the Authorization Server token call).

Request

URL: POST https://api.handelsbanken.com/mlurd/decoupled/mbid/cancel/2.0
Headers:
Content-Type: application/json
Accept: application/json
Body: { } empty JSON

Response

JSON parameters: { } empty JSON

The Authorization Server will always try to return 200 “OK” regardless if the cancellation was successful or not (except for initial failures).

Other changes

Token resource

There is a new path for the call:

Old URL: https://api.handelsbanken.com/bb/gls5/oauth2/token/1.0

New URL: https://api.handelsbanken.com/mlurd/oauth2/token/1.0

Authorize resource

TPPs that use the URL link that is returned at POST Consent, POST Payment etc. will not need to adjust anything as the new path will be returned.

Only TPPs that have hard-coded URLs (i.e. with the old path) need to adjust. Please do this is in good time and use the URL links that are returned instead.

Effect on POST Consent / POST Payment

During the grace period two links will be returned.


```
  "scaMethodType" : "DECOUPLED",
  "_links" : {
    "authorization" : [
      {
        "href" : "https://api.handelsbanken.com/bb/gls5/decoupled/mbid/initAuthorization/1.0",
        "name" : "decpld_mbid_1.0",
        "type" : "application/json"
      },
      {
        "href" : "https://api.handelsbanken.com/mlurd/decoupled/mbid/initAuthorization/2.0",
        "name" : "decpld_mbid_2.0",
        "type" : "application/json"
      }    ]    }
},
```