API INTERFACE ERP TO T24

Table of context

1. Introduction

1.1.General

The general access to account of ERP can be described in 3 main domains:
- ✓ Establishing a consent for Access to account information
- ✓ Account information
- ✓ Payment initiation

UBB uses API interfaces according to local standard BISTRA as subversion of Nextgen Access to account standard of Berlin Group. The interface is based on request/response principle. The direction is limited from ERP system to the bank resources. It means that only ERP system will initiate requests. The bank will response for success or not successful result.

In order to keep high level of security UBB apply Strong customer authentication approach via REDIRECT method to own webpage. In the cases of Authentication needed (Establishing consent and Payment initiation) the user will be redirected to UBB website in order to apply Strong Customer Authenticantion method. This procedure is identical with the internet banking login required passphrase and second factor for identification – OTP from Hardware token, OTP from software token or SMS.

1.2.Purpose

The purpose of this document is to describe the scope and business models of the solution, which will allow access of ERP to the bank system through the online services.

2. ERP Connectivity and validation

The secure connectivity is based on HTTPS protocol. The validation of the client application who initiate requests will be based on a valid Qualified Website Authentication Certificate (QWAC).

2.1.Certificate issuing

UBB strongly recommends his customers to use Organization Validation (OV) SSL Certificate. The main purpose of OV SSL certificate is to encrypt website/business and user's sensitive information which is being used for transactions. The certificate must be imported in ERP system in order to keep secure level of communication with UBB Openbanking solution.

2.2.Registration an OAuth application

UBB needs to receive the public part of the certificate. Once it received, UBB will register the application on behalf of the customer. In the process of registration the Client Id and Client Secret will be generated. UBB will send back to the customer this value keys. In addition UBB will subscribe the customer application for the respective API products.

2.3.Authentication the user via OAuth

The usage of OAuth2 requires authentication of a ERP customer in a pre-step, translating this authentication into an access token to be used at the API interface afterwards. In order to get Access token the customer should follow the steps in described scenario for Sandbox and Postman tool in https://developer.ubb.bg/ubb-sb/psd2/system/files/inline-files/Step-by-step_0.pdf.

UBB will provide to the customer all mandatory data required which must be used in the process of Get token:

- Access Token URL
- Client ID
- Client Secret
- Scope

The customer is mandated to import the private part (.pfx file) of his QWAC certificate in Postman tool with respective passphrase.
Before using any API, the customer must get Access Token with appropriate scope (consents, PSP_AI, PSP_PI). Once received, the Access token is valid for 60 minutes.

3. Scope and API business description

3.1.Consent for Access to account

The Consent creation is a mandatory condition that precedes the Account Information services. The user is obliged to first create a consent with the bank system, in which to indicate the accounts and the type of information he will consume (balances, transaction history or both).

API endpoints Consents

Link	Resource	Endpoints
Create consent	consents	POST /consents
Consent status request	consents	GET / consents /{ ConsentId }/status
Get Consent Request	consents	GET / consents /{ConsentId}
Delete Consent	consents	DELETE / consents /{ ConsentId }

The service includes the following scenarios:

- Create consent – this API is used to establish consent, defining access rights to dedicated accounts of a given user.
- Get consent status – Check the consent status, whether is valid or not
- Get consent – returns the details over the consent established
- Delete consent
- The detailed documentation, API description and test scenarios you can try here

According to BISTRA standard, the existing consent cannot be updated. If the customer needs to update the existing details, he must cancel (delete) the consent and create a new one.

3.2. Account Information

These activities allows the customer's application to retrieve information about the customer's accounts in accordance with the access data in the consent. UBB requires the use of existing APIs regarding:

API endpoints Account information

Link	Resource	Endpoints
Accounts	accounts	GET /accounts GET /accounts/{AccountId}
Balances	balances	GET /accounts/{AccountId}/balances
Transactions	transactions	GET /accounts/{AccountId}/transactions
Transaction Details	transactions	GET /{account-id}/transactions/{resourceId}

- Accounts list – the user is able to retrieve the list of all accounts consented
- Account details – the user is able to retrieve the detailed information over particular account consented with or without balance
- Account balances– the user is able to retrieve the various types of balances over concrete account consented
- Account Transaction list – the user is able to retrieve transaction history for certain period over particular account consented
- Account Transaction details - the user is able to retrieve the information over concrete transaction and particular account consented
- The detailed documentation, API description and test scenarios you can try here

3.3.Payment initiation

Users can initiate payments for execution by UBB. The payment initiation process follows the request / response principle. The response from the bank contains a link to the website where the payment with one or more signatures is authorized. The payment services provided to customers are described as follows:

1. Single payments

API endpoints Single payments

Link	Resource	Endpoints
Payment	domestic-credit-transfers-bgn domestic-budget-transfers-bgn sepa-credit-transfers cross-border-transfers	POST /{payment-product} GET /{payment-product}/{paymentId} GET /{payment-product}/{paymentId}/status

- Domestic credit transfer in BGN – this is transfer in local currency between UBB and other Bulgarian banks or intrabank payment
- Domestic budget transfer in BGN – this is a specific structured transfer in local currency in favor of state budget.
- SEPA credit transfer – Transfer in EUR to consumers, companies and other economic actors in Single euro payments area (SEPA). SEPA covers all EU countries, Iceland, Liechtenstein, Norway, Switzerland and Monaco.
- Cross border credit transfer - Transfer in foreign currency all over the world using SWIFT infrastructure.

2. Bulk payments API endpoints - Exclusively for customers with ERP systems
   - Bulk payment domestic credit transfers in BGN – Array with credit transfers in local currency
   - Bulk payment domestic budget transfers in BGN – Array with transfers in local currency to government budget structures
   - Bulk payment SEPA credit transfers – Array with SEPA credit transfers

API endpoints Bulk payments

Link	Resource	Endpoints
bulk-payments	domestic-credit-transfers-bgn domestic-budget-transfers-bgn sepa-credit-transfers	POST /{payment-product} GET /{payment-product}/{paymentId}/status

3. Get status of single payment
4. Get payment information of single payment
5. Get status of bulk payment
6. The detailed documentation, API description of single payments and test scenarios you can try here.

3.4. Postman collections and Test environment

UBB is ready to support the most valued customers in order to make more easy the preparation and implementation in production their API application based on ERP. Regarding this, UBB provides to their customers dedicated Test environment, Postman collections and Test certificate. UBB is ready to help its customers prepare their API infrastructure in a test environment, as close as possible to the production environment.

3.5. Authorization on the UBB Online SCA webpage

This service is the last point in the request/response journey of the create consent and payment initiation. This is where UBB applies a Strong Customer Authentication (SCA) mechanism to the end user. UBB provides the scaRedirect link in the APIs for Create Consent and Initiate Payment. The user application must use this link and redirect its customer. The processes of user identification and payment authorization are keeping the schema rules in electronic banking. This procedure is mandatory point for Consent approval and every Single or Bulk Payment authorization.