PSD2 – Fallback Option for API channel Bancabadell & Main channel for international offices

Version: 2.0

19/05/2021

Sabadell

Table of Contents

Introduction

Objective

This document outlines the way in which TPPs will be able to access the Banco Sabadell portals in compliance with the PSD2 directive.

TPP

A TPP (Third-Party Provider), Financial Provider, AISP or PISP acts on behalf of a payment service user by accessing its banking information at another entity or initiating a transfer. It requires a licence from an NCA, and it can operate in other countries by virtue of the "passport" concept by making use of eIDAS certificates.

Web scraping

Web scraping is a method used by third parties to access customers' information which is shared with the bank and use it for their own purposes. This method is based on the automation of the access to the online banking website used by the bank's customers.

These accesses using the web scraping technique must be self-identified by means of the use of an eIDAS certificate which identifies the third party who is accessing the information on the bank's customers.

The EBA has published several documents that outline the use of these kinds of certificates for use by the different TPPs.

Requests for access

In accordance with the PSD2 regulations, a TPP wishing to gain access by means of secure web scraping must indicate which portals it wishes to access, identifying itself as an authorised TPP with their name and company name and providing the appropriate eIDAS certificates:

- a QWAC certificate that can authenticate it as an entity
- a QSEAL certificate for the signing of the messages to be sent to the portals on which the TPP wishes to perform the web scraping.

Access

URL of the portals

A list of the addresses accessible using web scraping is provided below:

Test environments

Portal	URL
BANCO SABADELL	https://pre.webapi.bancsabadell.com/cs/Satellite/SabAtl/
ACTIVOBANK	https://pre.webapi.activobank.com/cs/Satellite/BC/
PARIS	https://pre.webapi.bancosabadellparis.com/cspre/Satellite/BSParis
UK	https://pre.webapi.bancosabadelluk.com/cspre/Satellite/BancoSabadellUK/
PORTUGAL	https://pre.webapi.bancosabadellportugal.com/BSLisboa

Productive environments

Portal	URL
BANCO SABADELL	https://webapi.bancsabadell.com/cs/Satellite/SabAtl/
ACTIVOBANK	https://webapi.activobank.com/cs/Satellite/BC/
PARIS	https://webapi.bancosabadellparis.com/cs/Satellite/BSParis
UK	https://webapi.bancosabadelluk.com/cs/Satellite/BancoSabadellUK/
PORTUGAL	https://webapi.bancosabadellportugal.com/BSLisboa

Requirements

The following requirements must be met to access the portals using web scraping:

1. The connection must be performed with an **HTTPS** protocol.

2. The authorised **QWAC** certificate must be submitted to execute the customer authentication upon access to the portal.

3. The **token** must be included in all the requests sent to the portal.

Token

A string must be generated with the parameters required by the portal operation to be invoked, signing the string with the QSEAL certificate and transforming the result into a B64 format. The result will be the token to be sent. Each of the steps is outlined below:

1. Generation of the parameter string to be sent

   To make valid requests, it is necessary to generate a token that must be sent in different ways, depending on the portal to be invoked:

   a. Paris and London

The string is generated by concatenating the input parameters of the operation to be invoked, in alphabetical order using its name, with the "&" separator and using the "=" character as a link between the parameter's name and value.

Example: *j_password=1234&j_username=12345678*

An empty string must be generated in the case of an HTTP request without parameters.

b. Activo Bank and Banco Sabadell

Like the Paris and London portals, the parameters of the operation must be concatenated, sorting them alphabetically by their names, using the "&" character as a separator of the name-value pairs and "=" to join the parameter's name and value together.

However, in the case of these portals, a urlPath=url parameter must always be added to the string (this url being that of the operation to be invoked) and "https" must be replaced by "http". For example, if the https://pre.webapi.bancsabadell.com/txbs/LoginDNISCA.doLogin.bs operation were to be attacked, the &urlPath=http://pre.webapi.bancsabadell.com/txbs/LoginDNISCA.doLogin.bs parameter must be added to the string, abiding by the alphabetical order.

c. Lisbon

In the case of the Lisbon portal, the string with the operation's parameters must be a JSON, given that it's a REST API. For example:

{"userId":"xxxxxxxx","pin":"xxxxx"}

2. Signature

Once the parameter string corresponding to each operation and portal has been generated, it must be signed using the private key of the QSEAL certificate that has been previously delivered, using the **SHA256withRSA** algorithm.

3. Transformation into B64

The next necessary step is to encode the result of the signature in Base64.

4. Delivery

The result of the Base64 encoding must be used as a token in the requests made to the portal under the name "TPPsignature".
This token will have to be sent in different ways, depending on the portal:

d. Lisbon

This token must be sent under the name “TPPsignature” as an HTTP header to the request.

e. Other Portals

This token must be sent under the name “TPPsignature” as a parameter that is sent in the body of the POST request.

In the event that the signature is generated incorrectly, the TPPsignature token is missing, the certificate isn’t installed because it hasn’t been requested, or the correct one hasn’t been used, the request will be rejected.