PSD2 – Fallback Option para Canal API BancSabadell y Canal principal para oficinas internacionales

Versión: 2.0

19/05/2021

Sabadell

Índice de contenido

Introducción

Objetivo

El presente documento describe la forma en que los TPP podrán acceder a los portales de Banco Sabadell en cumplimiento con la directiva PSD2.

TPP

Un TPP (*Third Party Provider*), Prestador Financiero, AISP o PISP, actúa en nombre de un usuario de servicios de pago accediendo a su información bancaria en otra entidad o iniciando una transferencia. Requiere una licencia por parte de una NCA y puede operar en otros países en virtud del concepto de "pasaporte" haciendo uso de certificados eIDAS.

Web scraping

Web scraping es la forma que los terceros utilizan para acceder a la información de los clientes compartidos con el banco y utilizarla para sus objetivos. Este método se basa en la automatización del acceso al site de la banca online que utilizan los clientes del banco.

Estos accesos mediante la técnica de web scraping deberán ser autoidentificados mediante el uso de un certificado eIDAS, el cual debe permitir conocer la identidad del tercero que está accediendo a la información de los clientes del banco.

La EBA ha publicado diferentes documentos que describen la utilización de este tipo de certificados para el uso por parte de los diferentes TPPs.

Solicitud de acceso

De acuerdo con la normativa PSD2, un TPP que desee tener acceso mediante web scraping secrizado debe indicar cuales son los portales a los que desea acceder, identificándose como TPP autorizado con su nombre, razón social y aportando los certificados eIDAS oportunos:

- certificado QWAC que servirá para autenticarse como entidad
- certificado QSEAL para la firma de los mensajes que se enviarán a los portales en los cuales el TPP quiere efectuar webscrapping.

Acceso

URL de portales

A continuación, se presenta un listado de las direcciones accesibles mediante web scraping:

Entornos pruebas

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

Entornos productivos

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

Requerimientos

Para acceder a los portales mediante web scraping se deben cumplir los siguientes requerimientos:

1. La conexión debe realizarse con protocolo **HTTPS**.

2. Se debe presentar el certificado **QWAC** autorizado para ejecutar la autenticación de cliente en el momento de acceso al portal.

3. Incluir el **token** en todas las peticiones ejecutadas al portal.

Token

Se debe generar una cadena con los parámetros requeridos por la operación del portal que se desea invocar, firmar esa cadena con el certificado QSEAL y transformar el resultado a B64. Este resultado será el token que enviar. A continuación, se detallan cada uno de los pasos:

1. Generación de la cadena de parámetros a enviar

   Para efectuar peticiones validas es necesaria la generación de un token que deberá ser informado de forma distinta en función del portal que se quiera invocar:

a. Paris y Londres

La cadena se genera concatenando los parámetros de entrada de la operación a invocar, en orden alfabético mediante su nombre, con el separador '&' y utilizando el carácter '=' como unión entre el nombre del parámetro y su valor.

Ejemplo: *j_password=1234&j_username=12345678*

En el caso de ser una petición HTTP sin parámetros, igualmente se debe generar una cadena vacía.

b. Activo Bank y Banco Sabadell

De igual forma que para los portales de Paris y Londres, se deben concatenar los parámetros de la operación, ordenándolos de forma alfabética por su nombre, utilizando el carácter '&' como separador de las parejas nombre valor y con '=' para unir el nombre y el valor del parámetro.

Sin embargo, en el caso de estos portales debe añadirse siempre en la cadena un parámetro urlPath=url, siendo esta url la de la operación a invocar, pero sustituyendo https por http. Por ejemplo, si se quiere atacar a la operación https://pre.webapi.bancsabadell.com/txbs/LoginDNISCA.doLogin.bs, deberá añadirse a la cadena, siguiendo el orden alfabético, el parámetro &urlPath=http://pre.webapi.bancsabadell.com/txbs/LoginDNISCA.doLogin.bs.

c. Lisboa

En el caso del portal de Lisboa, la cadena con los parámetros de la operación debe ser un JSON, ya que se trata de una API REST. Por ejemplo:

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

2. Firma

Una vez generada la cadena de parámetros correspondiente a cada operación y portal se debe firmar utilizando la clave privada del certificado QSEAL que se haya entregado con anterioridad, utilizando el algoritmo **SHA256withRSA**.

3. Transformación a B64

El siguiente paso necesario es el de codificar el resultado de la firma en Base64.

4. Envío

El resultado de la codificación en Base64 deberá ser utilizado como token en las peticiones que se efectúen contra el portal, con el nombre firmaTPP.

Este token deberá ser informado de distinta manera dependiendo el portal:

d. Lisboa

Este token debe ser informado con el nombre firmaTPP como una cabecera HTTP de la petición.

e. Resto de Portales

Este token debe ser informado con el nombre firmaTPP como parámetro que se envíe en el body de la petición POST.

En el caso de que la generación de la firma sea incorrecta, o no venga el token firmaTPP, o no se encuentre el certificado instalado por no haber sido solicitado, o no se haya utilizado el correcto, la petición será rechazada.