

PSD2

CaixaBank, S.A, está desarrollando una adaptación de la interfaz de la sucursal de Polonia para dar acceso a proveedores de servicios financieros (TPP y CBPII) y para que utilicen dicha interfaz para la autenticación y comunicación con los usuarios de servicios de pago (PSUs).

La solución se está desarrollando con el objetivo de cumplir con los requisitos y funcionalidades establecidos por el Reglamento RTS, en la fecha establecida del 14 de septiembre de 2019 (Reglamento Delegado (UE) 2018/389 con respecto a las normas técnicas de regulación para la autenticación fuerte de clientes y las normas comunes y securización de los estándares abiertos de comunicación” (“Reglamento RTS ”).

El Reglamento RTS requiere el uso de certificados eIDAS para la identificación de TPP. Las especificaciones de eIDAS están incorporadas en la norma ETSI TS 119 495.

Todas las solicitudes a las cuentas de los PSUs deben estar firmadas para garantizar la identificación de TPP. Las firmas HTTP proporcionan un método de autenticación y, además, verifican que la comunicación entre el cliente y el servidor no ha sido alterada. Este enfoque está siendo estandarizado por el IETF.

Los TPPs deberán seguir los siguientes pasos para firmar correctamente la solicitud:

- 1. Uso del certificado de firma:** se requiere un certificado eIDAS QSEAL emitido por un proveedor de servicios de confianza cualificado.
- 2. Creación del Digest:** se debe generar un hash codificado en base64 de las cabeceras HTTP de la solicitud. Está pendiente de confirmación los métodos de algoritmo hash permitidos y, los componentes finales que formarán el digest, también están pendientes de definir.
- 3. Cadena de firma:** la cadena de firma que contiene las cabeceras de fecha y el digest debe crearse. Está pendiente confirmar si se agregarán otras cabeceras a la cadena.
- 4. Firmar con clave privada:** la cadena de firma obtenida en el paso anterior se firmará con la clave privada.
- 5. Creación de la cabecera de la firma:** la cabecera de la firma que se añade a la solicitud contendrá la cadena firmada obtenida en el paso 4. Está pendiente definir los componentes finales que formarán parte de la cabecera de la firma.