Documentación Canal de Fallback

Documentación canal de Fallback

Objeto

El presente documento recoge la propuesta tecnológica para proveer de un mecanismo de autenticación en el acceso a los canales digitales de CaixaBank con llamadas a los dominios:

- CaixaBankNow Web: https://lo.caixabank.es
- CaixaBankNow Móvil: https://lo.caixabank.es

Propuesta tecnológica

Siguiendo el estándar de identificación 'Signing HTTP Messages' de 'Cavage & Sporny' (https://tools.ietf.org/html/draft-cavage-http-signatures-11) se propone utilizar el timestamp de las peticiones (header Date) de la ejecución como el campo a firmar. Este mínimo firmado permitirá comprobar la autenticación del certificado EIDAS.

Proceso de firma para una Request

1. Utilice su certificado eIDAS QSEAL (PSD2) emitido por el proveedor de servicios de confianza calificado de su elección.

2. Crear la string de firma

   La cadena de firma contiene cómo mínimo la cabecera Date, que es el mínimo permitido por el estándar, pero también es conveniente introducir un RequestID para fortalecer la autenticación.

   por ejemplo: date: Sun, 05 Jan 2014 21:31:40 GMT

3. Crea la cadena de firma y firme con RSA y la clave privada del certificado de firma.

   El algoritmo de firma y resultado debería ejecutar el siguiente algoritmo BASE64(RSA-SHA256(cadenaFirma))

   SjWJWbWN7i0wzBvtPl8rbASWz5xQW6mcJmn+ibttBqtifLN7Sazz6m79cNfwwb8DMJ5cou1s7uEGKKCs+FLEEaDV5lp7q25WqS+lavg7T8hc0GppauB6hbgEKTwblDHYGEtbGmtdHgVCk9SuS13F0hZ8FD0k/5OxEPXe5WozsbM=

4. Generar la cabecera de firma que consiste en los siguientes componentes:

KEID	Número de serie de PSD2 eidas QSEAL
Algorithm	Especificar el algoritmo usado en la generación de la firma. El primario es el rsa-sha256
Headers	La lista de las cabeceras que contienen o se han utilizado para la firma: • minúsculas • Separadas por un espacio • En el mismo orden que se ha utilizado en la cadena de firma En el caso de usar sólo la cabecera date se puede obviar.
Signature	El resultado del punto 3

5. El resultado del punto 4 se debe introducir en la cabecera Authorization.

Authorization: Signature keyId="Test",algorithm="rsa-sha256", headers=”date", signature="SjWJWbWN7i0wzBvtPl8rbASWz5xQW6mcJmn+ibttBqtifLN7Sazz6m79cNfwwb8DMJ5cou1s7uEGKKCs+FLEEaDV5lp7q25WqS+lavg7T8hc0GppauB6hbgEKTwblDHYGEtbGmtdHgVCk9SuS13F0hZ8FD0k/5OxEPXe5WozsbM="

O

Signature keyId="Test",algorithm="rsa-sha256", headers=”date", signature="SjWJWbWN7i0wzBvtPl8rbASWz5xQW6mcJmn+ibttBqtifLN7Sazz6m79cNfwwb8DMJ5cou1s7uEGKKCs+FLEEaDV5lp7q25WqS+lavg7T8hc0GppauB6hbgEKTwblDHYGEtbGmtdHgVCk9SuS13F0hZ8FD0k/5OxEPXe5WozsbM="

6. Se solicita incluir la parte pública del certificado EIDAS en la petición de login, para poder realizar el proceso en el menor tiempo posible. En el resto de peticiones es factible introducir la URL donde comprobar o descargar el certificado.

```
"tpp_signature_certificate":"-----BEGIN PUBLIC KEY-----
\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCFENGw33yGihy92pDjZQhl0
C36rPJj+CvfSC8+q28hxA161QFNUd13wuCTUcq0Qd2qsBe/2hFyc2DCJJg0h1L78
+6Z4UMR7EOcpfdUE9Hf3m/hs+FUR45uBJeDK1HSFHD8bHKD6kv8FPGfJTotc+2xj
JwoYi+1hqp1fIekaxsyQIDAQAB\n-----END PUBLIC KEY-----"
```

7. Se genera la petición incluyendo las cabeceras http indicadas, e incluyendo en el user agent de la petición una identificación clara NombreTPP – URL;

Flujo de acceso

A continuación, se detalla el flujo de acceso:

1. Primer acceso
    a. Mediante los datos identificativos indicados en el apartado “Proceso de firma para una Request”, se realiza el login del TPP para un cliente.
    b. En el caso que sea el primer login del TPP identificado para el cliente, se procederá a solicitar SCA (strong Customer Authentication), el cual, dependerá del mecanismo de firma que tenga configurado el cliente.
    c. En el caso que el SCA sea satisfactorio, se realizará la asignación de confianza necesaria entre el acceso del TPP y el Cliente por el canal de fallback.
    d. Con la asignación de confianza, sólo se solicitarán los SCA necesarios

2. Siguientes accesos
    a. En los siguientes accesos del TPP identificado no se solicitará SCA en el momento de login. En la sesión se podría llegar a solicitar SCA en aquellas operativas donde sea necesarios por normativa, seguridad y/o prevención de fraude.

NOTA: En el caso que el usuario revoque los accesos al TPP autenticado, o por motivos de renovación, se volverá a solicitar SCA en el momento del login para volver a asignar la confianza necesaria entre TPP autenticado y cliente.

Anexos

1. Signing HTTP Messages draft-cavage-http-signatures-11
   https://tools.ietf.org/html/draft-cavage-http-signatures-11#page-10
2. https://w3c-dvcg.github.io/http-signatures/