Documentació sobre el canal de *fallback*

Documentació sobre el canal de *fallback*

Objectiu

Aquest document recull la proposta tecnològica per a proveir d'un mecanisme d'autenticació en l'accés als canals digitals de CaixaBank amb crides als dominis:

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

Proposta tecnològica

Seguint l'estàndard d'identificació 'Signing HTTP Messages' de 'Cavage & Sporny' (https://tools.ietf.org/html/draft-cavage-http-signatures-11), es proposa utilitzar el *timestamp* de les peticions (*header Date*) de l'execució amb el camp que se signa. Aquest mínim signat ha de permetre comprovar l'autenticació del certificat EIDAS.

Procés de signatura per a una *request*

1. Utilitzi el certificat eIDAS QSEAL (PSD2) que emet el seu proveïdor de serveis de confiança qualificat.

2. Creï l'*string* de signatura

   La cadena de signatura conté com a mínim la capçalera *Date*, que és el mínim que permet l'estàndard, però també és convenient introduir un *RequestID* per a enfortir l'autenticació.

   per exemple: date: Sun, 05 Jan 2014 21:31:40 GMT

3. Creï la cadena de signatura i signi amb l'RSA i la clau privada del certificat de signatura.

   L'algorisme de signatura i resultat hauria d'executar l'algorisme següent: BASE64(RSA-SHA256(cadenaSignatura))

   SjWJWbWN7i0wzBvtPl8rbASWz5xQW6mcJmn+ibttBqtifLN7Sazz6m79cNfwwb8DMJ5cou1s7uEGKKCs+FLEEaDV5lp7q25WqS+lavg7T8hc0GppauB6hbgEKTwblDHYGEtbGmtdHgVCk9SuS13F0hZ8FD0k/5OxEPXe5WozsbM=

4. Generi la capçalera de signatura, que consta dels components següents:

KEID	Número de sèrie de PSD2 eidas QSEAL
Algorithm	Especificar l'algorisme que s'utilitza en la generació de la signatura. El primari és l'rsa-sha256
Headers	La llista de les capçaleres que conté o que s'han utilitzat per a la signatura: • minúscules • separades per un espai • en el mateix ordre que s'ha utilitzat en la cadena de signatura En el cas que s'utilitzi només la capçalera *date*, es pot obviar.
Signature	El resultat del punt 3

5. El resultat del punt 4 s'ha d'introduir a la capçalera *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 sol·licita incloure la part pública del certificat EIDAS a la petició de *login*, per a poder efectuar el procés en el temps més curt possible. En la resta de peticions, és factible introduir l'URL en què es pot comprovar o descarregar el certificat.

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

7. Es genera la petició incloent les capçaleres http indicades i incloent en el *user agent* de la petició una identificació clara (NomTPP – URL);

Flux d'accés

A continuació, es detalla el flux d'accés:

1. Primer accés
    a. Amb les dades identificadores que s'indiquen a l'apartat “Procés de signatura per a una *request*”, s'introdueix el *login* del TPP per a un client.
    b. En el cas que sigui el primer *login* del TPP identificat per al client, es procedeix a sol·licitar una SCA (*strong customer authentication*), que depèn del mecanisme de signatura que el client té configurat.
    c. En el cas que l'SCA sigui satisfactòria, l'assignació de confiança necessària entre l'accés del TPP i el client es fa pel canal de *fallback*.
    d. Amb l'assignació de confiança, només se sol·liciten les SCA necessàries.

2. Accessos següents
    a. En els següents accessos del TPP identificat no se sol·licita cap SCA en el moment del *login*. En la sessió es podria arribar a sol·licitar una SCA en operatives en què siguin necessàries per normativa, seguretat i/o prevenció de frau.

NOTA: En el cas que l'usuari revoqui els accessos al TPP autenticat, o per motius de renovació, s'ha de tornar a sol·licitar una SCA en el moment del *login* per a tornar a assignar la confiança necessària entre el TPP autenticat i el client.

Annexos

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/