Fallback Channel Document

Fallback Channel Document

Object

This document includes the technological proposal for providing an authentication mechanism for accessing the digital channels of CaixaBank with calls to the domains:

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

Technological Proposal

Following the "Signing HTTP Messages" identification standard by "Cavage & Sporny" (https://tools.ietf.org/html/draft-cavage-http-signatures-11) it is suggested to use the timestamp of the request (Date header) in the signature parameters field. This signed minimum version will allow for verification of the authenticity of the EIDAS certificate.

Signature process for a Request

1. Use the eIDAS QSEAL (PSD2) certificate issued by the trusted service provider of your choice.

2. Create the signature string

   The signature string contains at minimum the header Date, which is the minimum allowed under the standard, but it is also convenient to enter a RequestID to strengthen the authentication.

   for example: date: Sun, 05 Jan 2014 21:31:40 GMT

3. Create the signature chain and signs with RSA and the private key of the signature certificate.

   The signature algorithm and result should implement the following algorithm: BASE64(RSA-SHA256(stringSignature))

   SjWJWbWN7i0wzBvtPl8rbASWz5xQW6mcJmn+ibttBqtifLN7Sazz6m79cNfwwb8DMJ5cou1s7uEGKKCs+FLEEaDV5lp7q25WqS+lavg7T8hc0GppauB6hbgEKTwblDHYGEtbGmtdHgVCk9SuS13F0hZ8FD0k/5OxEPXe5WozsbM=

4. Generate the signature header consisting of the following components:

KEID	Serial number of PSD2 eidas QSEAL
Algorithm	Specify the algorithm used in generating the signature. The primary is rsa-sha256
Headers	The list of header fields included or that have been used in generating the signature: • lowercased letters • separated by a single space • in the same order that was used in the signature string If only using the date heading this can be disregarded.
Signature	The result of point 3

5. The result of point 4 should be entered into the Authorization header.

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

   Or

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

6. It is requested to include the public part of the EIDAS certificate in the login request, to be able to carry out the process in the shortest time possible. For the other requests it is possible to enter the URL where the certificate can be downloaded or verified.

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

7. The request is generated with the HTTP headings indicated, and including a clear NameTPP – URL identification in the User-Agent;

Access Flow

The flow of access is detailed below:

1. First access
   a. Using the identification data indicated in the “Signature process for a Request” section, the TPP login is made for a client.
   b. If it is the first TPP login identified for the client, it will continue to request the SCA (strong Customer Authentication), which will depend on the signature mechanism the client has configured.
   c. If the SCA is correct, the necessary authentication will be made between the TPP access and the client using the fallback channel.
   d. With the authentication made, only the necessary SCA will be requested.

2. Subsequent access
   a. In the subsequent access of the identified TPP, the SCA will not be requested when logging in. During the session a request for SCA may be needed in the cases where it is necessary by law, security and/or fraud prevention.

NOTE: In the event that the user revokes the access to the authenticated TPP, or for updating reasons, the SCA will again be required at the time of login to provide the necessary authorization between the TPP and client.

Annexes

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/