PSD2 TPP AUTHENTICATION PRE-REQUISITE TO ACCESS FALLBACK SOLUTION ON "HELLOBANK.COM"

VERSION 1.2

Website for Hellobank Retail market in France

This documentation is based on the STET draft v1.4 "Fallback solution standard".

Contact : paris.bddf.support.api.dsp2@bnpparibas.com

BNP PARIBAS

La banque d'un monde qui change

1. PREAMBLE

This note intends to describe the mechanism applied by Hello bank! for identifying/authenticating a Third Party Provider (TPP) in the usage context of a fallback solution meeting the expectations of the final version of RTS on SCA.
This note does not address the authentication of the Payment Service user (PSU).

Versioning of this document:

- Version 1.0 – July 23, 2019
- Version 1.1 – October 30, 2019: add an example + SCA customer journey
- Version 1.2 – July 1, 2020: process to manage SCA (update)

2. CORE PRINCIPLES

The fallback solution to access PSU's live data is based on the specific authentication mechanism using signature that has to be processed, through a Qualified Electronic Seal Certificate (QSEALC), and forwarded by the TPP to Hello bank! for verification and authentication.

3. AUTHENTICATION PREREQUISITES TO ACCESS FALLBACK SOLUTION

This note is based on the IETF http-signature DRAFT.

- One must notice this is not an approved Request for Comment (RFC) yet.
- Moreover, the latest version on this draft has expired in November 2018.
- However two API initiatives consider this draft as stable enough to be part of their respective API specifications.

3.1 WORKFLOW

The initiation step of the workflow is the TPP accessing to the following resource (accessible after PSU authentication):
https://www.hellobank.fr/fr/client/mes-comptes/mes-avoirs/releve-d-operation (method: GET)
By requesting this resource, the TPP will compute a signature and add the relevant data as extra-http-headers.
By getting those extra-http-headers, the ASPSP can ensure that an identified TPP signed the request and therefore can reasonably assume that the request is indeed originated from this TPP.
The ASPSP can either immediately check the signature or save the provided data for further processing.
The ASPSP will then compute a Session Cookie that will be linked to both the PSU identity and the TPP identity and forward this Session Cookie to the TPP.
Until its expiration, the Session Cookie will allow the continuation of data exchanges between the TPP and the ASPSP.

3.2 DETAILED SIGNATURE MECHANISM

Content to be signed

- Core data

The TPP has to provide a timestamp that will be forwarded to the ASPSP as an extra-http-header whose name must be equal to:

- "tpp-signature-timestamp"

Important: Please note that your server time has to be NTP synchronized.

- ETSI Authorization Number

Following the ETSI TS119495 Technical Specification and for allowing a quick identification processing of the TPP, the later must add an extra-http-header containing the Authorization Number as present in the Organisation Identification of its QSEALC.

The extra-http-header name must be:

- "tpp-etsi-authorization-number".

Signature processing

Applying the IETF http-signature DRAFT specification, the TPP will compute the signature on the previously listed extra-http-headers. This signature must use:

- the private key linked to the TPP QSEALC;
- a strong-enough (at least RSA-SHA256) signature algorithm.

The TPP must also compute a key identifier that will help to retrieve the QSEALC. It is required that:

- the keyId is an http/https URL to the QSEALC;
- the QSEALC can be retrieved in a PEM format;
- the last part of the URL is suffixed by an underscore followed by the base64 representation of the fingerprint of the QSEALC.

Eventually, the TPP will add an extra-http-header containing:

- the key identifier;
- the algorithm that was used;
- the list of headers that were signed;
- the signature result itself.

The extra-http-header name must be:

- "signature".

Important: the signature will be valid during 60 seconds after the timestamp generation.

3.3 INTERACTION EXAMPLE

curl https://www.hellobank.fr/fr/client/mes-comptes/mes-avoirs/releve-d-operation
-H 'Connection: keep-alive'
-H 'Upgrade-Insecure-Requests: 1'
-H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36'
-H 'Sec-Fetch-User: ?1'
-H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
-H 'Sec-Fetch-Site: same-origin'
-H 'Sec-Fetch-Mode: navigate'
-H 'Referer: https://www.hellobank.fr/fr/client/mes-comptes/mes-avoirs/releve-d-operation'
-H 'Accept-Encoding: gzip, deflate, br'
-H 'Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7'
-H 'Cookie: WCM_SESSIONID=...
-H "tpp-signature-timestamp: 1565191718"
-H "tpp-etsi-authorization-number: PSDFR-ACPR-51514"
-H "signature: keyId=^\^"https://path.to/myQsealCertificate_612b4c7d103074b29e4c1ece1ef40bc575c0a87e^\^",algorithm=^\^"rsa-sha256^\^",headers=^\^"tpp-signature-timestamp tpp-etsi-authorization-number^\^",signature=^\^"ny8dUFiW9B0NBhylZa+NQf3tHVkjtMRvExfbnXps5NkN+dVDqetfp5MBmmwXIS4/eNNYxXp4m/1ct5AdDulCNyu9PeVDii2a2Nv2NXE5YGN8SF/R/io4tmIpoYTDUxPqR6IrhUGB2Jcso1ibx0bwGXgFjp9EPniAFaLBBAipasY=^\^"" –compressed

4. SCA CUSTOMER JOURNEY

Hello bank! offers two strong authentication solutions to its customers:

- Clé Digitale (based on an enrolled smartphone and the validation of notification sent on the banking app)
- One Time Password received by SMS

The activation of one or the other solution depends on the client's equipment.
You will find below the SCA customer journey available.

The process described below corresponds to the BNP Paribas screens but the journey is exactly the same for Hello bank!.

A. AUTHENTICATION PHASE WITH "CLÉ DIGITALE"[1]

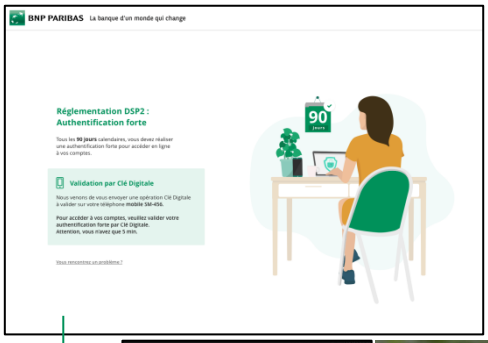
Client Identification (Desktop) & Authentication process (on App)

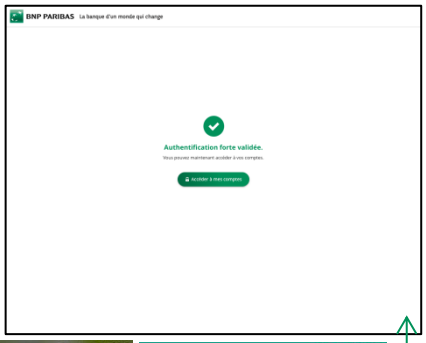
- Fill the Banking ID field and the secret code

The user receives a notification on the banking app to proceed to the authentication process;

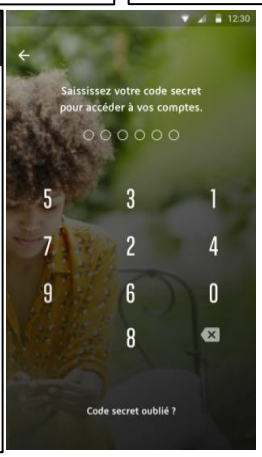
- The user clicks on the "Valider" button and then enters his secret code BNP Paribas;
- Once this step is completed the user can access his online banking.

DESKTOP





PHONE



[1] The displays shown serve as illustratives only

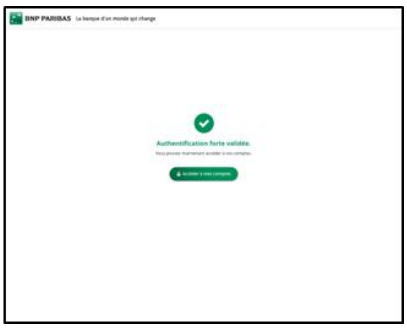
4.2 AUTHENTICATION PHASE WITH "OTP SMS"[2]

Client Identification (Desktop) & Authentication process (Mobile + Desktop)

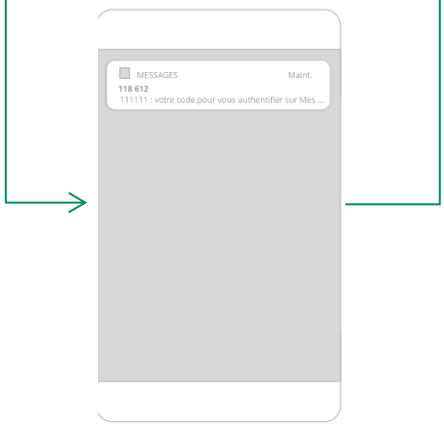
- Fill the Banking ID field and the secret code
- The user receives an OTP via SMS on his mobile to proceed to the authentication process;
- The user fills the code on the dedicated field on the desktop and clicks on the "Valider" button;

Once these two steps are completed the user can access his online banking.

DESKTOP



PHONE



[2] The displays shown serve as illustratives only

5. PROCESS TO MANAGE SCA

Step 1: Login as usual

- Banking ID field and secret code

Step 2: Detect the SCA

After filling the secret code a redirection will occur with a location to https://www.hellobank.fr/fr/client/authentification-forte. Just check this URL on 302 status requests.

Step 3: Ask to send the OTP

- For this step, call https://www.hellobank.fr/identification-wspl-pres/askAF, with:
  - POST method
  - Cookies of the current session
  - Empty JSON body {}

  Status must be 200, if not, an error has been made in your implementation.

Check the answer of the previous request to find out the authentication method the user has chosen.
It must be a JSON. Two cases:

- SMS mode

ex:

```
{
  "codeRetour": 0,
  "data": {
        "infosDeclenchementAF": {
              "numTel":"*******5142",
              nbreEssaiOtp:"2"
        },
        "modeAF":"02"
  }
}
```

- App validation mode (“Clé digitale”)

ex:

```
{
  "codeRetour": 0,
  "data": {
        "infosDeclenchementAF": {
              "device":"IPhone X"
         },
        "modeAF":"01"
  }
 }
```

You can rely on the presence of the numTel (SMS mode) or of the device (app validation mode) fields or trust the value of the modeAF field (“01” = app validation mode, “02” = SMS mode).

Step 4: Validate the OTP

Once the user fills the SMS code or confirms the operation with his mobile app, validate using https://www.hellobank.fr/identification-wspl-pres/validateAF, with:

- POST method
- Cookies of the current session
- JSON body {'otp': '<the_code>'} if SMS mode, empty JSON body if app validation mode

Status must be 200, if not, an error has been made in the implementation.

Step 5: Treat the response

- The previous request gives a JSON response. 2 cases:

a) There is a field 'message' in the JSON response, that means that the authentication failed (user put the wrong OTP, the service is unavailable etc...). The message is typically one of:

i. *Code saisi incorrect.*
➔ user put an incorrect SMS code.

ii. *Validation par clé digitale en attente.*
➔ user did not validate the operation in his mobile app, you need to redo step 4) until the field message disappears.

iii. *Validation par clé digitale expirée.*
➔ user did not validate the operation in his mobile app, and it is too late to complete the challenge (5 minutes timeout).

iv. *Service (actuellement) indisponible.*
➔ This may occur if you do not ask the SMS code but try to validate it. A random error is not excluded too.

b) There is no field 'message' in the JSON response, that means the authentication succeeded. In that case, just resend any request to https://www.hellobank.fr with the same cookies and you will be able to access the user accounts.