PSD2 TPP AUTHENTICATION PRE-REQUISITE TO ACCESS FALLBACK SOLUTION ON "MABANQUEENTREPRISE.BNPPARIBAS"

VERSION 1.2

Website for BNP Paribas Corporate 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

The bank
for a changing
world

1. PREAMBLE

This note intends to describe the mechanism applied by BNP PARIBAS 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 18, 2019 : add a video about Secure Browsing
- Version 1.2 – October 30, 2019 : add an example

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 BNP PARIBAS 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 connecting to mabanqueentreprise.bnpparibas and accessing the resource "GET https://secure1.entreprises.bnpparibas.net/sommaire/jsp/identification.jsp".

By requesting this form, 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, in a ISO 8601 representation, 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://secure1.entreprises.bnpparibas.net/sommaire/jsp/identification.jsp"
-H "Connection: keep-alive"
-H "Cache-Control: max-age=0"
-H "Upgrade-Insecure-Requests: 1"
-H "User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36"
-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 "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: psetimeout_was8=1565173394171; sso_session_id_was8=SSO_LOGIN;
TS015fe314=018f08081bf14e45ade26de4185037b1bdb94de2e1845ae885fd49946d7a5286ddfd5560ae53cc06c9aea96498a
f5efb258bb1a5abd0c3e4cc754491aa27216736603a29ba;
TS01423422=018f08081b9c9ab70b4e9f3e224b8c164f529cae5d0c1474defc8cb2b3ff1243491adbfaad1625b6f708b689befbb
bfa56bcbc2a99; PSEm=MTAuMTg2LjIyOC4xMjg=; __utma=70242194.1959732379.1565171590.1565171590.1565171590.1;
__utmc=70242194; __utmz=70242194.1565171590.1.1.utmcsr=(direct)^|utmccn=(direct)^|utmcmd=(none);
JSESSIONID=0000P_BEq-b9AMMJSATLoB2MLao:1apvcp0jn;
TS01aa4de0=013dee356ea1be62477680dcf7dafad0d9f1a4e746b3e8c95d5081ce5e68030e89ddb6404d4d352821a2f77ab2a
000a14d4a719cc2f314454660d5894857aadc2b79c89a80ca36c625f58c873cab9aebb2594234091ab3bfe3a5a303ef52144b9
6f27df493ac894ae029ab39ee9cf638a9a58b44c291a51cb9d1d57e711db70af9c8bb6890"
-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/1
ct5AdDulCNyu9PeVDii2a2Nv2NXE5YGN8SF/R/io4tmIpoYTDUxPqR6IrhUGB2Jcso1ibx0bwGXgFjp9EPniAFaLBBAipasY=^\^"" –
compressed
```

4. A NEW ACCES MEAN: "SECURE BROWSING"

In order to better protect their access from their computer, tablet or smartphone, users will have to register their web browser.

Please see an overview in the Secure Browsing Video

If the above link is not clickable, try copying and pasting it into the address bar of your web browser:
https://dam.bnpparibas.com/vcm2/php/playerExterne.php?file=vcm_1567603573041_-4565071203088152313.mp4&nr=workspace://SpacesStore/e477e270-2dc0-4bd8-9609-0ceb503f0af5