DOCUMENTATION TPP : FALLBACK DOCUMENTATION – DEVELOPERPORTAL HOWTO

Version du 23/11/2020
Référence DSB : SB-INF-20172

GENERAL PURPOSE

By the Revised Payment Services Directive [PSD2], Account Servicing Payment Service Providers (ASPSPs), are required to grant Third Party Payment Services Providers (TPPs) - conditionally on the requirements of the PSD2 and the RTS - access to their customers' (Payment Service User's – PSU) bank accounts.

For this purpose, ASPSPs implement dedicated interfaces through which TPPs access the ASPSPs administration system and, thus, the PSU bank accounts. The dedicated interface allows the ASPSP not only to identify the TPP by certificates, but provides a secure access environment to protect PSU data. With respect to the dedicated interface's performance and availability, the EBA asks ASPSPs to monitor both and provide contingency (fallback) mechanisms in case the dedicated interface is unavailable. Therefore, in agreement with the regulator, a fallback mechanism is temporarily made available by the ASPSP until the dedicated APIs are in place.

DESCRIPTION

The proposed fallback solution consists of a Guest book service, carrying out regulatory controls required by the EBA, before redirecting the TPP to the ASPSP Home Banking site. These controls correspond to:

- TLS MA 1.2 resolution (mutual authentication) with the TPP during each exchange
- Verification that the certificate's CA is an official QTSP of the EU Trusted List (https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers)
- Verification that the certificate is not revoked by QTSP via Certificate Revocation List (CRL).

TPPs **are required** to register in the Guestbook prior to each session (each AIS or PIS request initiation) in order to perform these regulatory controls.

The Fallback session is represented by a unique identifier (called **REQUEST_ID**) which is provided by the Guestbook and which identifies the session. The **REQUEST_ID** is valid for 10 minutes and the TPP must persist it on their side and provide it in the scrapping request. A Session is defined as follow :

- AIS : Account consultation initialization transaction : a session is a scrapping period of maximum 10 minutes
- PIS : Payment initiation workflow – A session is defined for each payment transaction.

For auditing purposes, the unique **REQUEST_ID** linked to the TPP will be tracked by the ASPSP.

OFFICE DES POSTES ET TÉLÉCOMMUNICATIONS DE NOUVELLE-CALÉDONIE (EPIC de la Nouvelle-Calédonie)
Direction des Services Bancaires - Immeuble Waruna II - 2 rue Paul Montchovet - 98841 Nouméa Cedex - Nouvelle-Calédonie
Centre Financier de Nouméa - téléphone (+687) 268800 - cfn@opt.nc - RCS Nouméa 2002 B132 720 - RIDET 132 720 001
www.ccp.nc

All these verification requests will be stored and tracked by the Guestbook. Once all checks have been carried out and validated by the bank's verification service the TPP will be redirected to the Home Banking site (using http 30X redirect) and will be able to perform "web-scrapping" on the html content as the TPP currently does.

It is the responsibility of the TPP to:

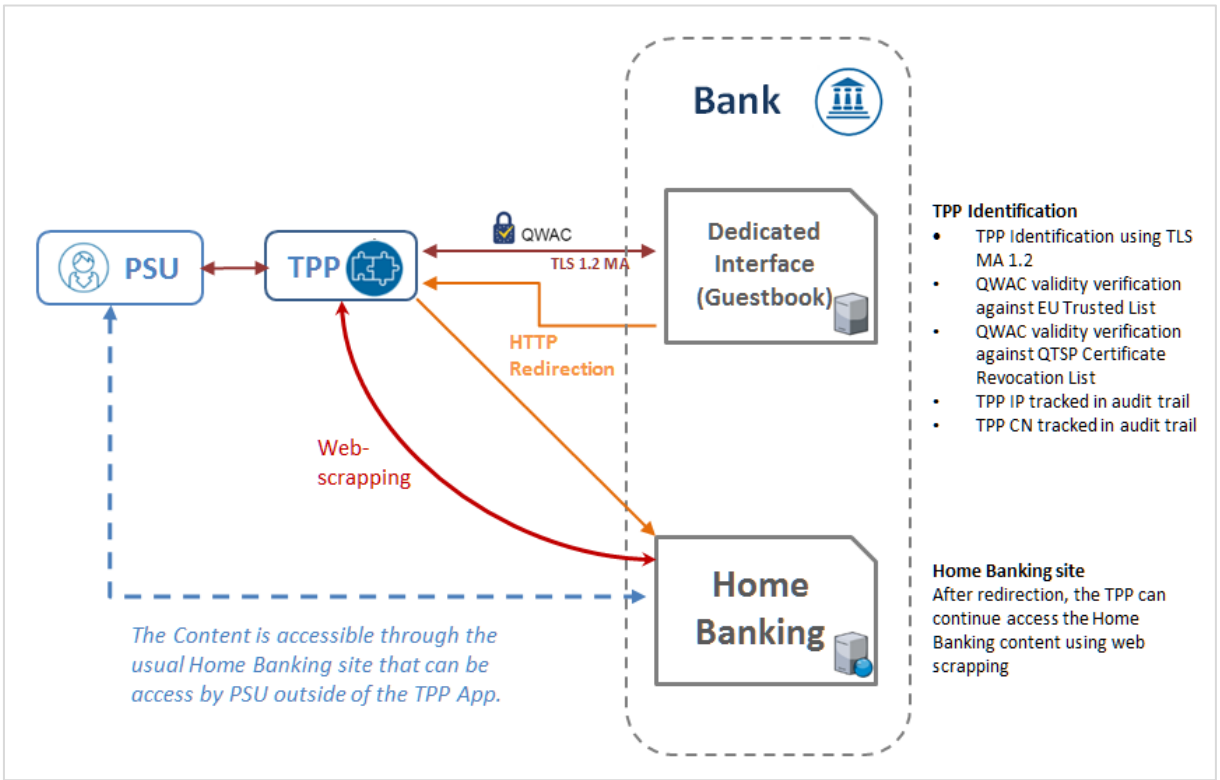
- Respect the fallback process and the RTS (including the limit of 4 AIS workflow without the PSU involvement in a period of 24h).
- Scrapp only the payment accounts for which the PSU gave his consent. The TPP is not allowed to scrapp other existing accounts of the PSU.

The ASPSP will be able to identify fraudulent TPP as TPP offering connection to the Bank service without being visible in the audit trail of the Fallback solution.

HOW TO CONNECT TO THE FALLBACK SOLUTION

The URL of the Guestbook solution exposed by OPT-NC is : https://fallback.ccp.nc
The URL of the HomeBanking is : http://www.ccp.nc/

The communication between the TPP and the GuestBook solution is always secured by using a TLS-connection Mutual authentication using TLS version 1.2 which is initiated by the TPP.
The TLS-connection has to be established always including client (i.e. TPP) authentication.
For this authentication the TPP has to use a qualified certificate for website authentication (QWAC) which has to be issued by a qualified trust service provider according to the eIDAS regulation, and has to be issued from a production CA (Certificate Authority).
The content of the certificate has to be compliant with the requirements of the EBA-RTS and follow the ETSI TS 119 495 V1.2.1 (2018-11) technical specification.
For security and auditing purpose, the bank requires the client certificate to be presented within each request.



OFFICE DES POSTES ET TÉLÉCOMMUNICATIONS DE NOUVELLE-CALÉDONIE (EPIC de la Nouvelle-Calédonie)
Direction des Services Bancaires - Immeuble Waruna II - 2 rue Paul Montchovet - 98841 Nouméa Cedex - Nouvelle-Calédonie
Centre Financier de Nouméa - téléphone (+687) 268800 - cfn@opt.nc - RCS Nouméa 2002 B132 720 - RIDET 132 720 001
www.ccp.nc

Example of request / response :

The TPP have to call the fallback URL with a valid QWAC certificate.

curl -k -vvv --cert PUBLIC_QWAC_KEY.cer --key PRIVATE_QWAC_KEY.key https://fallback.ccp.nc
* Rebuilt URL to : https://fallback.ccp.nc
* ...
* Server certificate : **Bank certificate (QWAC)**
* ...
* SSL certificate verify ok.
> GET / HTTP/1.1
> Host : https://fallback.ccp.nc
> User-Agent: curl/7.54.0
> Accept: ***/***
>
< HTTP/1.1 **302 Moved Temporarily**
< ...
< Location : **https://ccp.opt.nc/fr/dciweb.htm?p0=idesai.tht&t=p?request_id=MTU2ODEwMzkwMDoxMC4wLjAuMTpQUORGUi1BQ1BSLVRQUC0yMjA4MTkxNzEyOlBTREZSLUFDUFItVFBQLTIyMDgxOTE3MTI6QUITLFBJUyxGQ1M=**
< ...
<html>
<head><title>302 Found</title></head>
<body>
...
</body>
</html>
* Connection #0 to host https://fallback.ccp.nc left intact

OFFICE DES POSTES ET TÉLÉCOMMUNICATIONS DE NOUVELLE-CALÉDONIE (EPIC de la Nouvelle-Calédonie)
Direction des Services Bancaires - Immeuble Waruna II - 2 rue Paul Montchovet - 98841 Nouméa Cedex - Nouvelle-Calédonie
Centre Financier de Nouméa - téléphone (+687) 268800 - cfn@opt.nc - RCS Nouméa 2002 B132 720 - RIDET 132 720 001
www.ccp.nc