PolishAPI

Recommendations and basic assumptions concerning the fall-back interface preparation

Document developed by the PolishAPI Project Group

08 July 2019
Version 1.0

Table of Contents

Table of Figures

1 Introduction and Reservations

The Commission Delegated Regulation (EU) No. 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (RTSs) obliges the payment account servicing payment service providers (ASPSPs) to develop fall-back measures concerning the special access interface. The fall-back measures comprise, but are not limited to, a description of the available fall-back interface.

Neither the PSD2 Directive nor the RTSs determine in detail the desired shape and way of operation of the fall-back interface. The limited regulatory requirements in this respect result from the provisions of Art. 33 (5) of the RTSs.

These *Recommendations and basic assumptions concerning the fall-back interface preparation* constitute a proposal of a joint and universal approach to the fall-back interface implementation, drawing upon the existing achievements of the Polish banking sector and the best market practices.

The recommendations and descriptions of assumptions contained herein are not binding both as regards their scope and extent. Also, they are not the only solutions possible that are admissible in the light of the legal requirements. At their discretion, at their own responsibility and based on the risk analysis carried out, the ASPSPs may take a decision to apply in whole or in part the recommendations and descriptions of assumptions as presented herein. This document does not constitute a legal opinion either.

The recommendations and descriptions of assumptions contained herein present the opinion developed during the work of the project group within the Polish Bank Association.

2 Assumptions

1. The first stage of the process is the verification of the QWAC certificate used to make the connection and the TPP's QSealC seal certificate.
2. The certificate verification is based on the verification of the QWAC and QSealC certificates provided in the headers. The verification also comprises an analysis of the certificate validity and structure as well as the TPP's rights to the PSD2 services. N.B.: The seal certificate verification, considering the potentially significant impact on the service efficiency without a critical impact on its security, may be deemed optional.
3. The client's authentication is based on the mechanism of redirection to the ASPSP's infrastructure.
4. The service is provided after the PSU's authentication and the provision of a token or a session ID so as to enable the TPP to provide the service on the client interface in accordance with the method selected by the ASPSP.
5. The AIS service provision without the PSU's participation is not covered by this recommendation and its provision depends on an individual decision of the ASPSP.

3 Payment Initiation Service (PIS) – process description

N.B.: The transfer data may be inserted before or after the PSU's authentication. It will entail a necessity to use a different process and a different process support.

1. The PSU launches the TPP's web application using a www browser. At this step, the PSU may also insert the transfer data.
2. The TPP's server starts connection with the fallback domain.<bank>.pl. The TPP provides the *tpp_redirect_uri* parameter containing the TPP's server address to which the PSU's browser will be redirected at the subsequent process steps.
3. Verification of the QWAC certificate used to make the connection and of the TPP's QSealC certificate*.
4. If the TPP's verification based on the certificates provided has been completed successfully, a *token** is generated and is used by the ASPSP to confirm the service provision. Additionally, URL leading to the address where the ASPSP's endpoint is located will be returned. In case of a negative verification of the TPP, the connection will be rejected.
5. The TPP redirects the PSU's browser to the web site of the ASPSP's electronic banking on the basis of URL received in the previous step.
6. The PSU authenticates itself at the ASPSP's electronic banking web site, providing its login data. Additionally, the ASPSP's electronic banking receives the *token* generated previously, which contains, without limitation, a confirmation of a successful verification of the TPP's certificates.
7. The ASPSP returns the *token* to the TPP.
8. Based on the *tpp_redirect_uri* parameter, the PSU is redirected to the web site of the TPP's application.
9. The TPP's server makes another connection with the ASPSP in order to collect the data of the session in the context of which the connection will be made.
10. The ASPSP provides the session data.
11. The TPP makes a connection with the electronic banking in the context of the PSU, using the session data received earlier in order to carry out the action on behalf of the PSU. This step may comprise the insertion of the transfer data.

The second authentication factor is inserted on the basis of three admissible methods as described in items 12, 13 and 14:

12. the *redirection* method, e.g. using the OTP (*One-time password*):
    a. the ASPSP generates an OTP and provides it to the PSU using an existing channel (e.g. using a text message);
    b. The PSU confirms the request / authorises the transaction in the ASPSP's interface. This method is transparent from the point of view of the TPP.
13. The *embedded* method, e.g. using the OTP (*One-time password*):
    a. the ASPSP generates an OTP and provides it to the PSU using an existing channel (e.g. using a text message);
    b. The PSU enters the OTP in the TPP's application;
    c. The TPP uses the code received to authorise the request / transaction.

14. The *decoupled* method (e.g. via a separate application of the ASPSP on a mobile device):

    a. the ASPSP generates an authorisation request and sends a *push* message to the mobile device;

    b. The PSU confirms the request / authorises the transaction. This method is transparent from the point of view of the TPP.

***service provided by the TSP (Technical Service Provider), it may also be provided by the ASPSP**

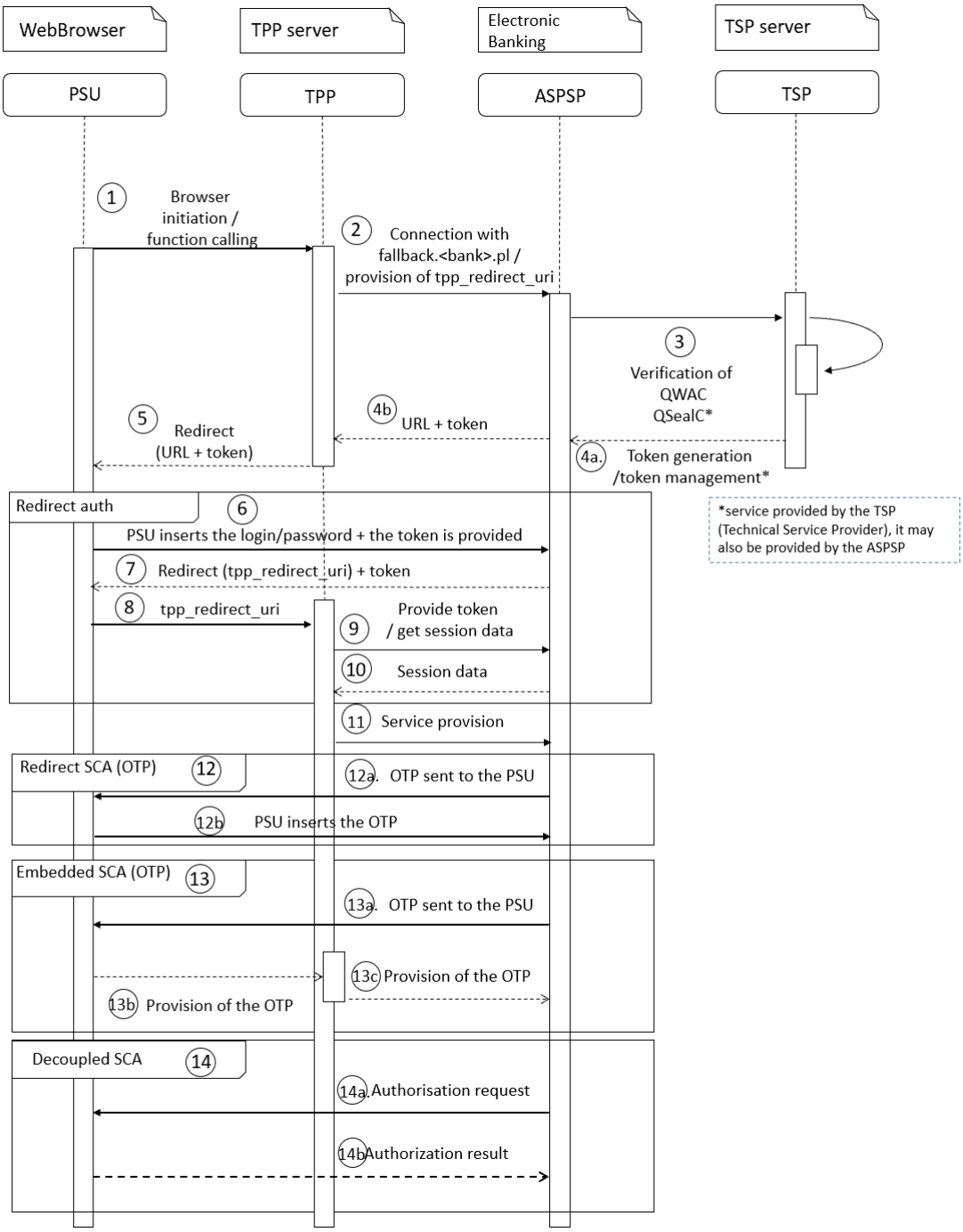

***Figure 1:** Payment initiation process*

4 Account information service (AIS) – process description

1. The PSU launches the TPP's web application using a www browser.
2. The TPP's server starts connection with the fallback domain.<bank>.pl. The TPP provides the *tpp_redirect_uri* parameter containing the TPP's server address to which the PSU's browser will be redirected at the subsequent process steps.
3. Verification of the QWAC certificate used to make the connection and of the TPP's QSealC certificate*.
4. If the TPP's verification based on the certificates provided has been completed successfully, a *token** is generated and is used by the ASPSP to confirm the service provision. Additionally, URL leading to the address where the ASPSP's endpoint is located will be returned. In case of a negative verification of the TPP, the connection will be rejected.
5. The TPP redirects the PSU's browser to the web site of the ASPSP's electronic banking on the basis of URL received in the previous step.
6. The PSU authenticates itself at the ASPSP's electronic banking web site, providing its login data. Additionally, the ASPSP's electronic banking receives the *token* generated previously, which contains, without limitation, a confirmation of a successful verification of the TPP's certificates.

The second authentication factor is inserted on the basis of three admissible methods as described in items 11, 12 and 13:

7. the *redirection* method, e.g. using the OTP (*One-time password*):
    a. the ASPSP generates an OTP and provides it to the PSU using an existing channel (e.g. using a text message);
    b. The PSU confirms the request / authorises the transaction in the ASPSP's interface. This method is transparent from the point of view of the TPP.
8. The *embedded* method, e.g. using the OTP (*One-time password*):
    a. the ASPSP generates an OTP and provides it to the PSU using an existing channel (e.g. using a text message);
    b. The PSU enters the OTP in the TPP's application;
    c. The TPP uses the code received to authorise the request / transaction.
9. The *decoupled* method (e.g. via a separate application of the ASPSP on a mobile device):
    a. the ASPSP generates an authorisation request and sends a *push* message to the mobile device;
    b. The PSU confirms the request / authorises the transaction. This method is transparent from the point of view of the TPP.
10. The ASPSP returns the *token* to the TPP.
11. Based on the *tpp_redirect_uri* parameter, the PSU is redirected to the web site of the TPP's application.
12. The TPP's server makes another connection with the ASPSP in order to collect the data of the session in the context of which the connection will be made.
13. The ASPSP provides the session data.
14. The TPP makes a connection with the electronic banking in the context of the PSU, using the session data received earlier in order to collect the data on behalf of the PSU.

***service provided by the TSP (Technical Service Provider), it may also be provided by the ASPSP**

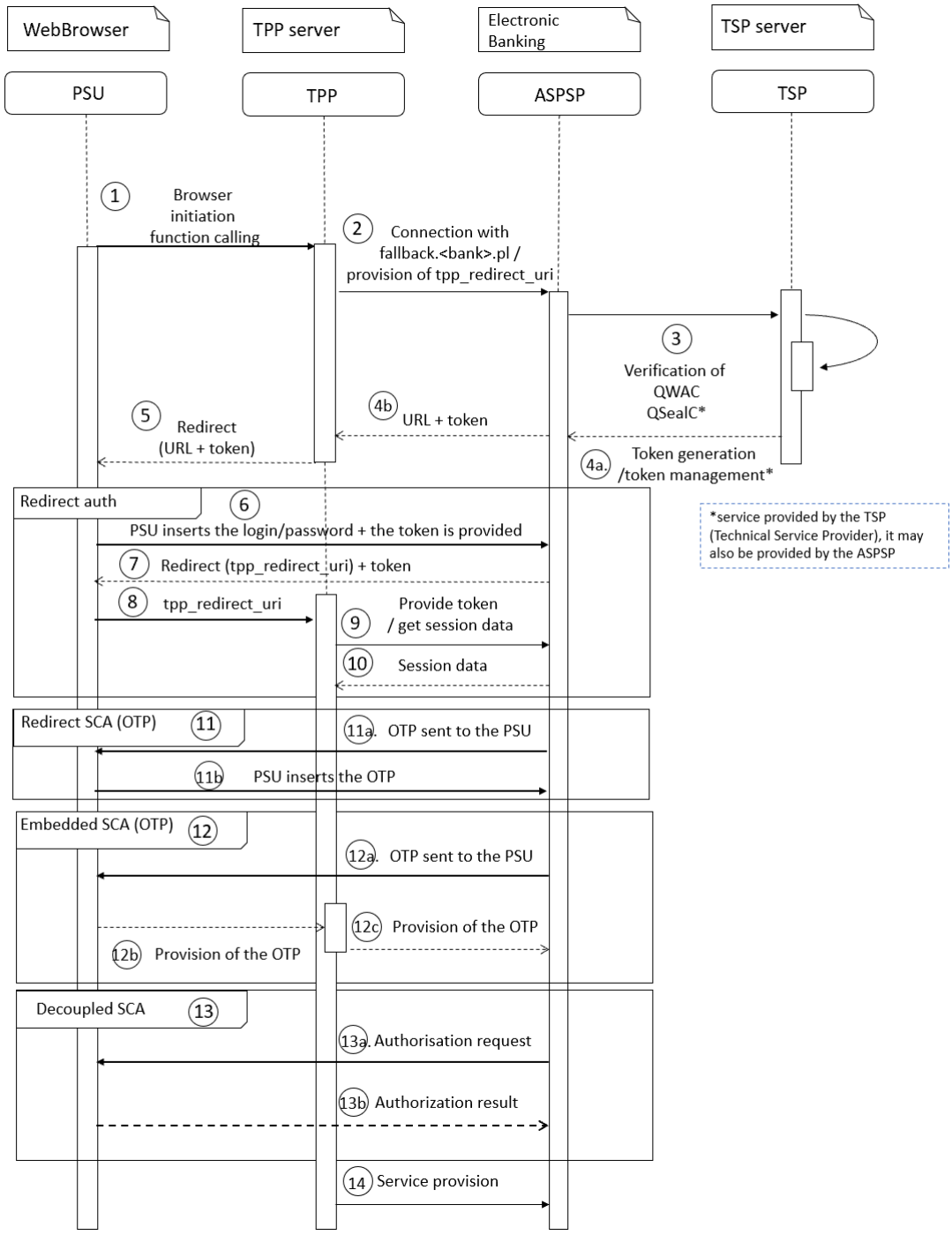

Figure 2: Account information process (with the PSU's participation)