PolishAPI

Recommendations and basic assumptions concerning the dedicated interface testing

Document developed by the PolishAPI Project Group

08 July 2019
Version 1.0

A description of activities to be performed on the TPP's side in order to confirm a correct testing of the ASPSP's API for compliance with the PSD2 Directive:

1. Making a connection by means of the Qualified Website Authentication Certificate (QWAC) compliant with the EIDAS* standard.
2. Signing of requests sent to the ASPSP. The Qualified Electronic Seal Certificate (QsealC)* is used to generate the JWS signature.
3. Verification of the QWAC and QSealC certificated of the ASPSP*:
    a. verification of the certificate's validity date;
    b. verification whether or not the certificate-issuing CAs are at the TSL's main list (narrowed down to CAs holding the accreditation to issue the QWAC and/or QsealC certificates);
    c. verification of the certificate's full path;
    d. verification whether or not the certificate has been annulled by checking the CRL list;
    e. (optionally) verification of the correct support of request rejects by API, if the certificate's PSD2 attributes do not authorise the TPP to use the given service.
4. Verification whether or not the JWS signature is authentic and has actually been generated by the ASPSP, to which the request was sent.
5. Establishment of a communications session with the Bank and obtaining the OAuth2 tokens in the following steps:
    a. send a request using the /authorize method. where, after a successful verification, an address will be returned in response under which the Internet banking service to which the PSU is authenticating is located;
    b. PSU's redirection to the address received and, after a successful authentication and redirection to redirect_uri, obtaining the auth_code parameter;
    c. support of the PSU's refusal to to grant a consent and other Internet banking errors (reverse redirection of the PSU's browser to the TPP);
    d. obtaining of the access_token and the refresh_token after the /token method has been called and provision of the auth_code held.
    e. use of the refresh_token to obtain a new access_token;
    f. (optionally) use of the exchange_token in order to obtain a new access_token with a changed scope of consents.
6. Verification of the API's correct support of request rejections in relation with the lack of consents or consent expiry.
7. Verification of the correct support by the API of rejections of those AIS requests that exceed the daily limits imposed by the directive.

8. Execution of all the PolishAPI methods the use of which is planned by the TPP (and to which it has the rights in relation with the roles assigned under the PSD2 Directive) and which are made available by the given ASPSP. The verification should in particular concern the following areas:
    a. verification whether all the fields required by the ASPSP in the methods used are sent in the requests;
    b. generation of a unique requestId;
    c. support of response paging;
    d. (optionally) support of the corporate client context;
    e. (optionally) the callback services.
9. The ASPSP's sandbox environment should ensure a communication with the TPP by means of tested QWAC and QSealC certificates compliant with the EIDAS standards in case the TPP does not have its own product certificates yet.

N.B. (*) The use and verification of the EIDAS certificates is an optional step in case of a sandbox environment; tests may be conducted irrespective of the business methods (5-8).

In the context of the EIDAS certificates used, it is recommended that the ASPSPs should allow for the following aspects in their documentations:

1. Definition of the maximum size of the http header that can be supported,
2. In the context of the use of the x5u header, it is expected that the url address given therein will support secure connections,
3. The expected value of the ‘kid’ header of the signature,
4. Examples of the signature calculation together with the expected fields.