Open Banking Europe Notes

on the EBA Obstacles to PSD2

1. Authentication procedures that Account Servicing Payment Service Providers' (ASPSPs) interfaces are required to support

The method that ASPSPs should support will depend on the methods made available by the ASPSP to the Payment Service User (PSU): redirect, decoupled or embedded. Biometrics should be supported by decoupled or app-to-app, transmitting the results of the biometric test.

The Bank's mobile app can be one of the two-factor Strong Customer Authentication (SCA) elements in an Account Information Service (AIS) or Payment Initiation Service (PIS) journey. All the authentication methods supported by the ASPSP must be included by the ASPSP in the API. Other additional or unnecessary steps may not be added. Any redirection or decoupled SCA must include a seamless redirect back to the AISP or PISP. This can include a mobile App.

2. Mandatory redirection at the point-of-sale

It is said that redirection (as the only SCA method) is a barrier in point of sale (POS) use cases. The EBA made clear that if the ASPSPs support other methods of SCA to the customer, there is no need to develop new authentication methods. This refers to cases where the mobile app could be used. However, a bank is not forced to build such a mobile App if they do not have one.

Nonetheless, if the ASPSP has found a way to allow its customers to initiate such a payment, then the same must be done via PIS.

3. Multiple SCAs

Multiple SCAs can be an obstacle. There must be no unnecessary steps in an AIS-only case. In a PIS journey, only a single SCA should be necessary if the PISP provides all the payment information, as no additional data is being given to the PISP.

Requiring two SCAs would be an obstacle unless the TPP accesses account information (e.g. a list of accounts) or initiates a payment from one of these accounts.

4. 90-days re-authentication

There are concerns that PSU must authenticate every 90 days, as this leads to negative impacts on the business. There is a suggestion that the TPP could authenticate on behalf of the PSU.

The EBA recalls that there is an exemption from the requirement to apply SCA for each access where the PSU or AISP accesses only a limited set of data. However, even under this exemption, PSUs are still required to re-authenticate every 90 days in order to confirm that the AISP can continue accessing the payment accounts data without SCA. This is a necessary requirement and urges that NCAs encourage ASPSPs to require SCA only every 90 days and not more frequently.

The EBA also recalls that SCA happens between the PSU and the ASPSP unless the ASPSP enters into an outsourcing relationship of some sort, which has its own requirements.

5. Account selection

There are queries about account selection under redirection with two models noted:

- The PSU selects their Account (IBAN) selection on the ASPSP domain.
- The PSU types in their account number on the ASPSP domain. This second one is considered as an obstacle to which the EBA agrees.

Different models are then discussed to avoid PSUs having to manually input their account details on an AIS or PIS journey:

- Use the AIS capability to bring backlists of accounts that can then be selected.
- Allow the PSU to select the account on the ASPSP domain when decoupled or redirect options are used. This latter does not work in an "embedded" approach and so if the PISP does not have an AISP license, they will have to require the PSU to manually enter IBAN information.

The EBA clarified that ASPSPs are not required (or even allowed!) to share the PSU account list with PISP only TPPs. For these reasons, not sharing the full list of accounts to a PISP is not an obstacle.

6. Additional checks on consent

There are questions on what constitutes an "additional check on consent" and opt-in procedures.

It is clear that it is the responsibility of the TPP to check consent and that the ASPSP “should not check that consent was given”. Therefore, a general ex-ante consent (“would you in the future like to use TPP services, or should we just block them for you”) is an obstacle.

But having said this, a PSU may instruct an ASPSP to restrict access to a specific TPP. In such case, ASPSPs should ensure that any restriction of TPPs’ access is done in compliance with the PSD2.

In the case of corporate accounts where the PSU is a legal entity, the EBA highlights that the ASPSP still cannot have additional checks when accessing via a TPP.

7. Additional registrations

Some TPPs reported that ASPSPs require additional registration. The EBA emphasises that “requiring additional authorisations or registrations is not allowed”.

Some technical registration may be required for secure communications (e.g. registering an app). This is not an obstacle if it does not create unnecessary friction in the customer journey. However, going beyond what is technically necessary is an obstacle (e.g. requiring contact details), as there can be an agreement to be part of such a registration process.

Mandatory registration steps with the ASPSP, in order for the TPP to identify the TPP beyond the eIDAS certificate, are an obstacle.