Question ID

2025_7607

Legal act

Directive 2015/2366/EU (PSD2)

Topic

Strong customer authentication and common and secure communication (incl. access)

Article

Article: 98

Paragraph

Paragraph: 1

Subparagraph

Letter: d)

COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations

Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication

Article/Paragraph

Article: 32; Paragraph: 3

Name of institution / submitter

ZNPay a.s.

Country of incorporation / residence

Czech Republic

Type of submitter

Other

Subject matter

Definition of "equivalent authentication procedure" for journeys initiated from a mobile application

Question

When a Payment Service User (PSU) initiates a service from a Third Party Provider's (TPP) mobile application, what is the correct "equivalent authentication procedure" of the ASPSP that should be used as the benchmark for assessing whether "unnecessary steps" have been added? Is it the ASPSP's mobile web browser authentication journey, or is it the ASPSP's native mobile banking application authentication journey?

Background on the question

Paragraph 15 of the EBA Opinion on obstacles (EBA/OP/2020/10) prohibits ASPSPs from adding "unnecessary steps" to the customer journey compared to the "equivalent authentication procedure" offered in their direct channels.

There is a significant ambiguity in practice as to what constitutes the "equivalent authentication procedure" when a service is initiated from a TPP's native mobile application. Many ASPSPs possess both a mobile web browser interface and a native mobile banking application, with the latter typically offering a much more seamless and user-friendly authentication experience (e.g., using biometrics without additional steps).

When a PSU initiates a journey from a TPP's mobile app, these ASPSPs often redirect the user to their mobile web browser journey. They then argue that any additional steps in this journey are compliant as long as they mirror the steps in their direct mobile web channel. This ignores the existence of their superior native mobile app channel. It is unclear which of the ASPSP's direct channels should serve as the correct benchmark for comparison in a mobile-to-mobile context.

Submission date

17/10/2025

Final publishing date

12/06/2026

Final answer

Article 32(3) of Commission Delegated Regulation (EU) 2018/389 requires account servicing payment service providers (ASPSPs) that have implemented a dedicated interface to ensure that the interface does not create obstacles to the provision of payment initiation and account information services.

As clarified in paragraphs 6, 7 and 15 of the EBA Opinion on obstacles under Article 32(3) of the RTS on SCA and CSC (EBA/OP/2020/10), the authentication procedure with the ASPSP as part of an AIS or PIS journey should not include unnecessary steps or require the payment service user (PSU) to provide unnecessary or superfluous information compared to the way in which the PSU can authenticate when directly accessing their payment accounts or initiating a payment with the ASPSP.

Paragraph 16 of that Opinion also clarified that if the PSU is using an AISP or PISP’s services via the AISP/PISP’s mobile app, ASPSPs that have implemented a redirection or decoupled approach and

that enable their PSUs to authenticate using the ASPSP's authentication app (a mobile banking app or a dedicated/decoupled app) to directly access their payment accounts or initiate a payment should enable that:

(i) the PSU is redirected from the AISP/PISP's app to the ASPSP's authentication app, without any additional and unnecessary steps in-between (such as the PSU being redirected first to the ASPSP's mobile browser environment); and that

(ii) after authentication with the ASPSP, the PSU is automatically redirected back to the AISP/PISP's app, without, for example, the PSU having to manually reopen the TPP's app, which would be an obstacle.

The assessment of whether unnecessary steps have been added must be based on a comparison with the way in which the PSU can authenticate when directly accessing their payment account or initiating a payment with the ASPSP. Accordingly, where a PSU uses the services of an AISP/PISP via an app provided by the AISP/PISP, and the ASPSP enables direct authentication via its mobile banking application, the relevant point of comparison is the ASPSP's mobile banking authentication procedure. In such circumstances, introducing additional steps in the AIS or PIS journey that are not part of the ASPSP's mobile app authentication procedure may constitute an obstacle within the meaning of Article 32(3) of the RTS.

By contrast, where the PSU initiates AIS or PIS in a mobile browser environment, and the ASPSP's authentication procedure available to PSUs is also performed via a mobile web interface, benchmarking against that mobile web authentication procedure would be appropriate.

Status

Final Q&A

Answer prepared by

Answer prepared by the EBA.
