

**Question ID**2025\_7606

---

**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**Clarification of the scope of the term "authentication procedures" in the context of the RTS and the EBA Opinion on obstacles

---

## Question

Does the term "authentication procedures" in the context of the EBA Opinion on obstacles (EBA/OP/2020/10) refer only to the final SCA method, or does it encompass the entire end-to-end user journey required to complete the authentication? Does this mean that any additional steps in the TPP flow, such as the need to click on a QR code image or manually enter a username to invoke the authentication app, which are not present in the direct channel, constitute a failure to support the same "authentication procedure"?

---

## Background on the question

Paragraph 14 of the EBA Opinion on obstacles (EBA/OP/2020/10) states that *"If the interfaces provided by ASPSPs do not support all the authentication procedures made available by the ASPSP to its PSUs, this would be a breach of Article 30(2) RTS and an obstacle under Article 32(3) RTS"*.

In practice, there is ambiguity as to the scope of the term "authentication procedures". Some ASPSPs appear to interpret this term narrowly, referring only to the final method of applying SCA (e.g., using biometrics or a PIN). However, these ASPSPs often prepend this final SCA method with a series of additional, cumbersome steps that are only present in the TPP journey. These steps can include requiring the PSU to click on a non-obvious QR code image on a web screen to invoke the app, or forcing the PSU to manually enter their username to trigger an authentication push notification.

These intermediary steps are not part of the authentication journey when the PSU accesses their account directly via the ASPSP's native mobile app. It is therefore unclear whether a journey containing such additional steps can be considered the same "authentication procedure" as the more seamless one in the direct channel.

---

## Submission date

17/10/2025

---

## Final publishing date

12/06/2026

---

## Final answer

Article 30(2) of the Commission Delegated Regulation (EU) 2018/389 provides that for the purposes of authentication of the payment service user (PSU), the interface referred to in Art. 30(1) of that Regulation must allow account information service providers (AISPs) and payment initiation service providers (PISPs) to rely on all the authentication procedures provided by the account servicing payment service provider (ASPSP) to the PSU.

Article 4(29) of Directive (EU) 2015/2366 (PSD2) defines authentication as 'a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials'.

Paragraph 7 of the EBA Opinion on obstacles under Article 32(3) of the RTS on SCA and CSC (EBA/OP/2020/10) clarified that the authentication procedure with the ASPSP as part of an AIS/PIS journey should not include unnecessary steps or require the 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. In the same vein, paragraph 15 of that Opinion further clarified that the authentication of the PSU with the ASPSP in an AIS/PIS journey, in a redirection or decoupled approach, should not create unnecessary friction or add unnecessary steps in the customer journey compared to the equivalent authentication procedure offered to PSUs when directly accessing their payment accounts or initiating a payment with the ASPSP.

The reference in the Opinion to the authentication procedure covers all actions required to verify the identity of PSU or the validity of the use of their specific payment instrument.

---

## **Status**

Final Q&A

---

## **Answer prepared by**

Answer prepared by the EBA.

---