

Single Rulebook Q&A

Question ID	2023_6767
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	97
Paragraph	-
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	30(2) and 32(3)
Date of submission	31/03/2023
Published as Final Q&A	29/09/2023
Disclose name of institution / entity	No
Type of submitter	Other
Subject matter	App to app redirection with biometrics for PIS
Question	Are ASPSPs required to offer redirected authentication with biometrics to users accessing their payment accounts through an AISP or initiating a payment through a PISP, if they offer redirected authentication with biometrics to users accessing accounts or initiating payments directly via the ASPSP?
Background on the question	A growing number of ASPSPs allow their users to authenticate using the ASPSP's dedicated authentication app as one of the two SCA factors categorised as possession when directly accessing their payment accounts or initiating a payment with the ASPSP. In these mobile payments use cases, the user is automatically redirected from the bank app to the dedicated authentication app, where biometrics satisfy the inherence criteria of SCA. However, these ASPSPs do not offer the same authentication procedure for users accessing accounts or initiating payments via an AISP or PISP. Instead, these users are only allowed to authenticate via an embedded or decoupled method and using manual input of account credentials - often involving a 6-12 digit number assigned by the ASPSP to the PSU which is difficult to memorise. The EBA has clarified in the Opinion on obstacles under Article

	<p>32(3) of the RTS on SCA and CSC (page 4) that if the interfaces provided by ASPSPs do not support all the authentication procedures made available by the ASPSP to its PSUs, that represents a breach of Art. 30(2) RTS and an obstacle under Article 32(3) RTS. Furthermore, the same EBA Opinion clarifies that “ASPSPs that enable their PSUs to authenticate using biometrics when directly accessing their payment accounts or initiating a payment, and that require the PSU to authenticate with the ASPSP to use AISPs/PISPs’ services, should also enable their PSUs to use biometrics to authenticate with the ASPSP in a PIS or AIS journey.”</p>
<p>Final answer</p>	<p>Article 30(2) of the Delegated Regulation (EU) 2018/389 (RTS on SCA&CSC) requires account servicing payment service providers (ASPSPs) to ensure that the access interfaces provided to account information service providers (AISPs) and payment initiation service providers (PISPs) in accordance with Article 30(1) of that Regulation do not prevent AISPs and PISPs from relying upon the authentication procedure(s) provided by the ASPSP to its payment service users (PSUs). As clarified in EBA Opinion on the implementation of the RTS on SCA&CSC (EBA-Op-2018-04), this means that the method(s) of carrying out the authentication of the PSU (i.e. redirection, decoupled, embedded or a combination thereof) that ASPSPs should support will depend on the authentication procedures made available by the ASPSP to its PSUs and should support all these authentication procedures.</p> <p>Furthermore, paragraph 12 of the EBA Opinion on obstacles under Article 32(3) of the RTS on SCA&CSC (EBA/OP/2020/10) clarifies that ASPSPs that enable their PSUs to authenticate using biometrics when directly accessing their payment accounts or initiating a payment, and that require their PSUs to authenticate with the ASPSP to use AISPs/PISPs’ services, should also enable their PSUs to use biometrics to authenticate with the ASPSP when using the services of an AISP or PISP.</p> <p>It follows from the above that ASPSPs offering redirected authentication with biometrics to PSUs accessing accounts or initiating payments directly via the ASPSP should also enable their PSUs to use biometrics to authenticate with the ASPSP when using the services of an AISP or PISP.</p>
<p>Link</p>	<p>https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2023_6767</p>

European Banking Authority, 03/10/2023
www.eba.europa.eu