Single Rulebook Q&A

Question ID	2021_6321
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	5
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
Date of submission	20/12/2021
Published as Final Q&A	27/01/2023
Disclose name of institution / entity	No
Type of submitter	Credit institution
Subject matter	Authentication procedures that ASPSPs' interfaces are required to support (using re-direction)
Question	In a pure redirection-based approach, can an ASPSP, which is not offering a mobile web browser to its PSU's, decide not to support an authentication via a mobile web browser authentication page (no app-to-mobile web browser or mobile web browser-to-mobile web browser redirection) for PISPs/AISPs on the basis of duly justified security risks, without being considered a breach of Article 97 (5) PSD2 and Article 30(2) of the RTS on SCA and CSC and/or an obstacle under Article 32(3) of the RTS on SCA and CSC?
Background on the question	Account servicing payment service providers (ASPSPs) are required to allow that payment initiation service providers (PISPs) and account information service providers (AISPs) rely on the authentication procedures provided by them to the payment service users (PSU) in accordance with Article 97 PSD2. Furthermore, Article 30(2) RTS requires ASPSPs to ensure that AISPs and PISPs can rely on all the PSU authentication procedure(s) provided by

an ASPSP to its PSUs. As clarified in EBA Opinions on the implementation of the RTS (EBA/OP/2018/04 and EBA/OP/2020/10), this implies that where the redirection method is used to carry out the authentication of the PSU, all the authentication procedures offered directly by the ASPSP to its PSUs should be supported also in a redirection scenario. If the interface provided by the ASPSP does not support all these authentication procedures, then this would be a breach of Article 30(2) RTS and an obstacle under Article 32(3) RTS. A possible interpretation of these rules leads to the consequence that, if a PSU is using the services of an AISP/PISP via either a mobile app or a mobile browser app provided by the latter, the ASPSP which has implemented a redirection should enable the PSUs to authenticate not only via the ASPSP's mobile app but also via an ASPSP's mobile browser authentication page. This means that ASPSP should provide not only an "app-to-app" redirection but also a "mobile app-to-mobile web browser" and a "mobile web browser -to-mobile web browser" redirection. "App-to-App" redirection allows the TPP to redirect a PSU from the TPP application to the ASPSP's mobile app, installed on the PSU's device, where the TPP can transmit details of the request and connect the PSU into the ASPSP app authentication screen or function. The PSU is then authenticated using the same authentication method (credentials) as normally used when the PSU directly accesses its account using the ASPSP's app (Soft OTP, pin-code or biometrics when activated). On the other side, in a "mobile app-to-mobile web browser" and a "mobile web browser -to- mobile web browser" redirection scenario, where the PSU does not have the ASPSP's mobile app, there should be a redirection to the ASPSP's mobile browser website so that the PSU can authenticate with the ASPSP, using the authentication method for a mobile web browser. Some ASPSPs have decided not to offer directly to their PSUs access to their electronic banking via mobile web browsers, due to duly justified security reasons. The question is whether in such a situation these ASPSPs are required to allow a redirection of the PSUs to an ASPSP's mobile web authentication page, which they consider as less secure. The duly justified security risks determining why some ASPSPs are reluctant to offer a mobile web browser authentication page are summarized here below: The security of a mobile app is much higher than the security of a mobile browser. Opening up a mobile browser environment leads to a decrease in security levels. Reasons: No access through 'insecure' systems. Access via rooted or jailbroken devices (smartphones and tablets) is blocked as these devices are more susceptible to malicious software. The mobile app contains software to detect whether a mobile device is jailbroken or rooted. It even detects if there is software installed to mask this. Bypassing the mobile app will prevent this check from happening and thus deny access. Lack of context information when using a mobile browser. Context information which is essential for a correct risk assessment. The mobile app collects a lot of contextual information about the device, such as the version of the OS, the patching level etc. which is considered during the risk analysis. When using a mobile browser this information is not available for fraud monitoring,

	which means the risk of abuse cannot be sufficiently assessed. Therefore, fraud monitoring will block requests initiated via a mobile browser more frequently. Mobile browsers are much more vulnerable to phishing, because the web address is normally not displayed. Many (publicly available) studies have been published on this subject. Because the ASPSP cannot have a contractual relationship with the AISP/PISP, the ASPSP has no legal possibility to require AISP/PIPSs to provide the necessary device profiling (such as the device fingerprint), that the ASPSP requires in its direct relationship with the PSU. Furthermore the EBA/OP/2020/10 of the 4th June 2020 on obstacles paragraph 16 and 17 states that where the PSU is using the AISP/PISP's services in a mobile web browser environment, and not via the AISP/PISP's app, this is not considered an obstacle if the PSU is redirected to the ASPSP's mobile browser authentication page to enter their credentials, provided that this is the only way in which PSUs authenticate when directly accessing their payment accounts via the ASPSP's mobile web browser environment. If we reverse this reasoning (a contrario reasoning) this means that if the PSU is using the AISP/PISP's services via the AISP/PISP's mobile app it should not be considered an obstacle if the PSU is redirected to the ASPSP's mobile app to enter its credentials, provided this is the only way in which PSUs authenticate when directly accessing their payment accounts via the ASPSP's mobile app. Argument that is further enhanced by the fact that this is the only way to provide secure access.
Final answer	Article 97(5) of Directive 2015/2366/EU (PSD2) requires account servicing payment service provider (ASPSPs) to allow payment initiation service providers (PISPs) and account information service providers (AISPs) to rely on the authentication procedures provided by the ASPSP to the payment service user (PSU). In line with Article 30(2) of the Commission Delegated Regulation (EU) 2018/389, ASPSPs should ensure that the access interfaces provided to PISPs and AISPs under Article 30(1) of the Delegated Regulation do not prevent PISPs and AISPs from relying upon the authentication procedure(s) provided by the ASPSP to its PSUs. As clarified in EBA Opinion on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04) and the EBA Opinion on obstacles under Article 32(3) of the RTS on SCA&CSC (EBA/OP/2020/10), this means that all the authentication procedures made available by the ASPSP to its PSUs in the ASPSP's direct customer channels need to be supported when an AISP or PISP is used. If they are not, this would constitute a breach of Article 30(2) of the Delegated Regulation and an obstacle to the provision of payment initiation and account information services under Article 32(3) of the Delegated Regulation. Furthermore, in accordance with Article 66(4)(c) and Article 67(3)(b) of PSD2, ASPSPs should treat payment orders transmitted through the services of a PISP, and respectively data requests transmitted through the services of an AISP without any discrimination, other than for objectively justifiable

	reasons. In line with paragraph 16 of the EBA Opinion on obstacles, 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 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; and (ii) that after authentication with the ASPSP, the PSU is automatically redirected back to the AISP/PISP's app. In the specific case described by the submitter in which the ASPSP does not offer its PSUs the possibility to directly access their payment accounts or initiate a payment via mobile web browsers, the PSD2 and the RTS do not require the ASPSP to enable PSUs to authenticate via a mobile web browser when an AISP or PISP is used. However, if the PSU is using the AISP/PISP's services via a mobile web browser, and the ASPSP does not offer its PSUs the possibility to authenticate via a mobile web browser authentication page when directly accessing their payment accounts or initiating a payment with the ASPSP, it will not be an obstacle if the PSU is redirected to the ASPSP's authentication app, provided that this is the only way in which PSUs can authenticate when directly accessing their payment accounts with the ASPSP. In such case, the ASPSP should, in line with paragraph 16 of the EBA Opinion on obstacles, enable that the PSU is redirected to the ASPSP's authentication app without any additional and unnecessary steps in-between and that after authentication with the ASPSP, the PSU is automatically redirected back to the AISP/PISP's page.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6321