Single Rulebook Q&A

Question ID	2021_6044
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(2)
Date of submission	21/06/2021
Published as Final Q&A	13/04/2022
Disclose name of institution / entity	No
Type of submitter	Credit institution
Subject matter	Re-engineering by TPP of the ASPSP's redirect API and PSU customer journey
Question	May a Payment Initiation Services Provider (PISP) connect to the dedicated interface of the ASPSP, only to subsequently embed ("screen scrape") the redirection approach into their own environment, without redirecting the PSU to the ASPSP's mobile banking app, for authentication? Are Third-Party Providers (TPPs) allowed to re-engineer the customer journey designed by the ASPSP to the effect that authentication of the PSU will take place in the TPP domain?
Background on the question	An Account Servicing Payment Service Provider (ASPSP) offers to Payment Initiation Services Providers (PISPs) a functioning redirect model, as part of a dedicated Application Programming Interface (API), meeting all requirements of EBA and local Competent Authority, both in relation to availability, performance and an obstacle free redirect approach where the ASPSP authenticates the Payment Service User (PSU) in the ASPSP domain. Are Third-Party Providers (TPPs) allowed to re-engineer the customer journey designed by the ASPSP to the effect that authentication of the PSU

	will take place in the TPP domain? A practice is noticed where PISPs connect to the ASPSP's API, and subsequently re-engineer the authentication flow (redirect flow) instead of directing the PSU to the ASPSP domain for authentication. In other words, a PISP uses a hybrid construction in which it connects to the ASPSP's PSD2 API, but subsequently intercepts the PSU redirect URL (aimed to lead to the ASPSP domain) and embedding the redirection flow directly into the PISP domain to perform screen scraping. ASPSPs that have opted for a redirect API generally have implemented such redirect API for the sake of security. The PISP can rely on the ASPSP's authentication procedures by the ASPSP performing Strong Customer Authentication (SCA) in its own domain. There are concerns about this circumvention of the redirect approach by PISPs or TPPs in general. Using the ASPSP's API yet manipulating/reverse engineering the (obstacle free) customer journey specifically designed by the ASPSP for SCA, is not only non-compliant with the RTS on SCA, but also creates confusion to PSUs and increases security and fraud risks. It is perceived that in case an ASPSP offers a fully functioning PSD2 API in combination with an obstacle free redirection approach there cannot be any legitimate reason for PISPs not to use such API in accordance with the ASPSP design thereof. Clarification on this matter is requested. Specific legislative provisions that support this: RTS SCA Article 31 allows ASPSPs to choose to implement a 'dedicated interface' over the alternative of 'allowing the PSP to use the PSU interface' PSD2 Article 97.5 and subsequently RTS SCA Article 30.2 require ASPSPs to make available to TPPs all authentication procedures it provides to its PSUs. This implies that the authentication methods (redirection, decoupled or embedded) which the ASPSP needs to make accessible to the TPP must be equal to the actual authentication procedures the ASPSPs have available to its PSUs. This also implies the use thereof by the TPP. Paragraph 48 of the EBA Opinion on the implementation of the RTS SCA and CSC of June 2018: In the cases of redirection and decoupled approaches, PSU's authentication data are exchanged directly between PSUs and ASPSPs, as opposed to embedded approaches, in which PSU's authentication data are exchanged between TPPs and ASPSPs through the interface.
Final answer	Articles 66(4)(a) and 67(3)(a) of Directive 2015/2366/EU (PSD2) prescribe that the account servicing payment service providers (ASPSP) shall communicate securely with payment initiation service providers (PISPs) and account information service providers (AISPs) in accordance with point (d) of Article 98(1) of PSD2. Article 30(3) of the Commission Delegated Regulation (EU) 2018/389 requires ASPSPs to ensure that 'the technical specification of any of the interfaces is documented specifying a set of routines, protocols, and tools needed by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments for allowing their software and applications to interoperate with

	the systems of the account servicing payment service providers'. Furthermore, in line with the clarifications provided in paragraph 48-50 of the Opinion on the implementation of the RTS on SCA&CSC (EBA-Op-2018-04) and paragraph 11 of the Opinion on obstacles under Article 32(3) of the RTS on SCA&CSC (EBA/OP/2020/10), ASPSPs are free to decide the methods of carrying out the authentication procedure of the payment service user (PSU), such as redirection, embedded or decoupled approaches (or a combination thereof), provided that they support all the authentication procedures made available by the ASPSP to their PSUs. Therefore, in accordance with Article 30(3) of the Delegated Regulation, PISPs and AISPs should follow the technical specifications set out by the ASPSP when accessing the ASPSP's interface. Where the ASPSP has opted for a redirection or a decoupled approach and does not allow in its documentation the possibility for the PISP/AISP to transmit the PSU's credentials to the ASPSP, the PISP/AISP should redirect the PSU to the ASPSP's domain to authenticate and should not introduce an approach for sending the PSU's personalised security credentials to the ASPSP that is different to the approach envisaged by the ASPSP in the technical specifications of the interface. Such latter approach would not be in line with the requirements of Article 30(3) of the Delegated Regulation.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6044

European Banking Authority, 14/04/2022
www.eba.europa.eu