Single Rulebook Q&A

Question ID	2021_6156
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	95
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	32 and 36
Date of submission	01/09/2021
Published as Final Q&A	27/01/2023
Disclose name of institution / entity	No
Type of submitter	Credit institution
Subject matter	Arbitrating between security and obstacles
Question	Can an Account Servicing Payment Service Provider (ASPSP) know a mobile phone number inside of the Third Party Provider (TPP)’s organisation in order to send a decryption password to the TPP out-of-band via SMS?
Background on the question	As a general principle of PSD2, security of operations is of utmost importance. To achieve security of operations, having a secured communication channel between Account Servicing Payment Service Provider (ASPSP) and Third Party Provider (TPP) for operational purposes (e.g. data exchange during TPP’s onboarding, or communication in case of an incident) can be of value. A simple way to realise this, is to encrypt those communications, and that the ASPSP sends a decryption password to the TPP out-of-band via SMS. This of course requires that the ASPSP knows a mobile phone number inside of the TPP’s organisation, which could be seen as an obstacle in the onboarding process, as it is not strictly necessary. This practice could be implemented, but it is not clear today for the financial institution, nor for its supervisory body if such an implementation would be inside of the boundaries of an acceptable interpretation.

Final answer	Article 32(3) of the Commission Delegated Regulation (EU) 2018/389 prescribes that 'account servicing payment service providers that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services. Such obstacles, may include, among others, preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers, imposing redirection to the account servicing payment service provider's authentication or other functions, requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of Directive (EU) 2015/2366, or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services.' Paragraph 50 of the Opinion on obstacles under Article 32(3) of the RTS on SCA&CSC (EBA/OP/2020/10) clarified that 'additional registrations required by ASPSPs for TPPs to be able to access the PSUs' payment accounts, or the ASPSPs' production interface, that go beyond what is technically necessary in order to ensure secure access to payment accounts under the conditions of the RTS, are an obstacle. For example, a requirement imposed by an ASPSP to TPPs to pre-register their contact details with the ASPSP in order for TPPs to have access to the ASPSP's API is an obstacle. This being said, a registration process that is optional, or that is agreed between the ASPSP and TPPs, is not an obstacle'. Accordingly, requiring TPPs to provide a mobile phone number to ASPSPs for submission of decryption password via an SMS is an obstacle.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6156

European Banking Authority, 30/05/2023
www.eba.europa.eu