Single Rulebook Q&A

Question ID	2021_6141
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	1
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	24
Date of submission	06/08/2021
Published as Final Q&A	17/12/2021
Disclose name of institution / entity	No
Type of submitter	Competent authority
Subject matter	Association of personalised security credentials to the payment service user
Question	Should strong customer authentication (SCA) elements always be issued under control of the Account service Payment Services Provider (ASPSP)?
Background on the question	When adding a payment card to a digital wallet, a payment service user is requesting the ASPSP for issuance of personalised security credentials to act as a possession element in future payment transactions. The process of adding the payment card to the wallet may have different options in the way the strong customer authentication for the association of the personalised security credentials according to Article 24 of Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication is executed. Some industry practices are observed where the wallet provider (in its role as token requester) provides certain SCA elements instead of the ASPSP. This could for example be a knowledge element for the payment service user which was issued and verified by the wallet provider. According to PSD2 Article 4(31), personalised security credentials are personalised features provided by the payment service provider to a payment service user for the purposes of authentication. According to EBA Q&A 2019_4827, the "tokenisation of card details may meet the requirements of

	Article 7(1) of the Delegated Regulation, if the payment service provider of the payer (the issuer) is involved in the process of issuance of the token directly or indirectly (e.g. through an outsourcing agreement with a third party, i.e. a token requestor such as a wallet provider in the case of digital wallets or a merchant in the case of cards on file).”
Final answer	Article 97(1)(c) of Directive 2015/2366/EU (PSD2) requires payment service providers (PSPs) to apply strong customer authentication (SCA) ‘where the payer carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. Article 4(31) of PSD2 defines ‘personalised security credentials’ as personalised features provided by the payment service provider to a payment service user for the purposes of authentication Article 24 of the Commission Delegated Regulation (EU) 2018/389 prescribes further that ‘payment service providers shall ensure that only the payment service user (PSU) is associated, in a secure manner, with the personalised security credentials, the authentication devices and the software’ and that ‘the association by means of a remote channel of the payment service user's identity with the personalised security credentials and with authentication devices or software is performed using strong customer authentication’. Accordingly, the payment service provider that has issued the payment card (issuer) is responsible for providing the SCA elements to the payment service user and is required to apply SCA when adding a payment card to a digital wallet. Finally, issuers may outsource the provision and verification of the elements of SCA to a third party. In that case, the issuer should comply with the general requirements on outsourcing, including the requirements of the EBA Guidelines on Outsourcing arrangements (EBA/GL/2019/02) and the applicable requirements of the Delegated Regulation, including Articles 6-8 in relation to the respective SCA element, and Article 3 in relation to the periodical review of the security measures.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6141