Single Rulebook Q&A

Question ID	2021_6145
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	9
Date of submission	31/08/2021
Published as Final Q&A	31/01/2023
Disclose name of institution / entity	No
Type of submitter	Credit institution
Subject matter	SCA applicability / Application of SCA at tokenisation stage
Question	Does the authentication to unlock the mobile device count as one of the elements of strong customer authentication when a payment service user is tokenising a card on an e-wallet solution such as Apple Pay?
Background on the question	Reference is made to Q&A_4827, where the EBA clarified that SCA should be applied at the time of the issuance of the token (the initial addition of the funding payment instrument) in accordance with Article 97(1)(c) of the PSD2. Would the SCA requirement be fulfilled if one element of SCA (possession) is present during the issuance of the token and the other element (knowledge (inputting of a PIN) or inherence (fingerprint or face recognition) would have been applied when the payment service user unlocked his mobile device?
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 6(1) of the Commission Delegated Regulation (EU) 2018/389 require PSPs to 'adopt measures to mitigate the risk that the elements of SCA categorised as knowledge are uncovered by, or disclosed to, unauthorised parties.' Article 8(1) of the Commission Delegated Regulation (EU) 2018/389 require PSPs to 'adopt measures to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties. At a minimum, the PSPs shall ensure that those access devices and software have a very low probability of an unauthorised party being authenticated as the payer.' Article 24(2)(b) of the Commission Delegated Regulation (EU) 2018/389 requires PSPs to apply SCA to associate by means of a remote channel the payment service user's identity with personalised security credentials. Q&A 6141 clarified that the PSP 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. Q&A 4047 also clarified that 'PSPs may outsource the execution of SCA to a third party. In that case, said PSPs should comply with the general requirements on outsourcing, including the requirements in the EBA Guidelines on Outsourcing arrangements (EBA/GL/2019/02). ' Q&A 4827 further clarified that 'SCA should be applied at the time of the issuance of the token' (adding a payment card to a digital wallet in order to create a token and associate it with the device). Accordingly, unlocking of a mobile phone with biometrics (e.g. a fingerprint) or with a PIN/password should not be considered a valid SCA element for the purpose of adding a payment card to a digital wallet if the screen locking mechanism of the mobile device is not under the control of the issuer or if the payer has not been associated previously through an SCA with the credential used for unlocking the phone.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6145