Single Rulebook Q&A

Question ID	2019_4637
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	28/03/2019
Published as Final Q&A	19/06/2020
Disclose name of institution / entity	No
Type of submitter	Other
Subject matter	Separation of factors for strong customer authentication
Question	If a mobile phone has two different e-banking apps on it, one for the banking agendas (a banking app where payments are initiated by entering password, possibly in combination with OTPs) and one for receiving the SMS OTPs (authorization app),would this scenario fulfill the PSD2 requirements of sufficient separation of both factors (since both factors reside on the same smartphone, but in different apps)?
Background on the question	There are different platforms for e-banking, such as using a PC/laptop and a mobile phone:Scenario 1:Using the PC interface to login to the bank, check one's account balance and initiate payments.When one logs into the bank one enters username and password into the browser of the PC (this corresponds to the factor "knowledge" according to PSD2).Since one needs a second factor to log into the account (e.g. "possession" according to PSD2), then one could use a smartphone, where the bank sends an SMS with a "One Time Password, OTP" to one's previously registered mobile phone.In this scenario the factors "knowledge" and "possession" are completely separated, since knowledge (static password) is input via the PC interface and the SMS is received on my Smartphone

	(possession).Scenario 2:Similar to Scenario 1, but use banking app on one's smartphone instead of the above mentioned PC interface.I.e. the same smartphone that is to be used for receiving the OTP.In this case the separation between "knowledge" and "possession" is not as strict as for the PC based e-banking GUI(i.e. only one hardware device is used, i.e. my smartphone for both "possession" and "knowledge").In the context of PSD2, is the separation between "knowledge" and "possession" still to be considered satisfactory, even though both factors use the same hardware device?[This could be viewed as a satisfactory separation of the requirements of PSD2.]Scenario 3:Building on scenario 2, one could use the same Banking app on one's smartphone to (1) enter username, (2) enter static password and (3) receive an OTP.Now the separation of factors is even worse compared to scenario 2, since the same hardware and the same app is used for both factors.Again: Is the separation between "knowledge" and "possession" still to be considered satisfactory?[This could be viewed as an unsatisfactory separation between factors]
EBA answer	In accordance with Article 9(1) of the Delegated Regulation (EU) 2018/389, "payment service providers (PSPs) shall ensure that the use of the elements of strong customer authentication (SCA) … is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the others". In addition, Article 9(2) requires PSPs to "adopt security measures, where any of the elements of SCA or the authentication code itself is used through a multi-purpose device to mitigate the risk which would result from that multi-purpose device being compromised". Article 9(3), in turn, provides that "…the mitigating measures shall include each of the following: (a) the use of separated secure execution environments through the software installed inside the multi-purpose device; (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party; (c) where alterations have taken place, mechanisms to mitigate the consequences thereof." It follows from the above that a one-time password evidencing possession used together with a knowledge element on the same multi-purpose device (e.g. a smartphone) may constitute a valid strong customer authentication and thus be compliant with the requirements of the Delegated Regulation, provided that the PSP has put in place measures to ensure that the breach of one of the elements does not compromise the reliability of the other element.

	Paragraph 26 of the EBA Opinion on the elements of SCA under PSD2 provides further details on when a mobile app can evidence possession.
Link	https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4637

European Banking Authority, 09/08/2020
www.eba.europa.eu