Single Rulebook Q&A

Question ID	2019_4532
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	Article 98
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	Recital 4
Date of submission	11/02/2019
Published as Final Q&A	24/07/2020
Disclose name of institution / entity	Yes
Name of institution / submitter	Quali-Sign LTD
Country of incorporation / residence	United Kingdom
Type of submitter	Other
Subject matter	Strong Customer Authentication (SCA) possession element requirement for cryptographic validation
Question	For a device to be considered possession:- a) should the device perform "cryptographically underpinned validity assertions using keys or cryptographic material stored in" the device? b) should the device be in the physical possession of the Payment Service User (PSU)? I.e. it cannot be held and operated remotely.
Background on the question	The following statements could potentially be interpreted in a contradictory manner:Recital 4 of the RTS states "Dynamic linking is possible through the generation of authentication codes which is subject to a set of strict security requirements. To remain technologically neutral a specific technology for the implementation of authentication codes should not be required. Therefore

	authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material STORED IN the authentication elements, as long as the security requirements are fulfilled."Opinion 35 of the EBA Opinion Paper states "Given that knowledge is defined as ‘something only the user knows’, the card number with CVV and expiry date printed on the card cannot be considered a knowledge element. This is also the case for a user ID. For a device to be considered possession, there needs to be a reliable means to confirm possession through the generation OR RECEIPT of a dynamic validation element on the device."In the case of a SIM card being considered as a possession element, Opinion 35 could be interpreted as that it is sufficient for the SIM to RECEIVE a code. However, Recital 4 suggests that on receipt of a code, the SIM must then perform a "cryptographically underpinned validity assertion".
Final answer	This question is related to the possession elements under Article 7 of the Delegated Regulation (EU) 2018/389, and not to the requirements on authentication codes or dynamic linking specified under Articles 4 and 5 of this Delegated Regulation. However, Recital 4 of the Delegated Regulation, to which the submitter refers, is related to authentication codes under Article 4 of the Delegated Regulation and not to possession elements. Recital 4 provides example of potential ways in which the authentication code can be designed without prescribing a specific technology for the implementation of authentication codes. In accordance with Article 4(30) of Directive 2015/2366/EU (PSD2), possession is ‘something only the user possesses’. Article 7 of the Delegated Regulation further specifies that ‘payment service providers (PSPs) shall adopt measures to mitigate the risk that the elements of strong customer authentication (SCA) categorised as possession are used by unauthorised parties’ and that ‘the use by the payer of those elements shall be subject to measures designated to prevent replication of the elements’. Paragraph 35 of the EBA Opinion on the implementation of the RTS on strong customer authentication and secure communication (EBA-Op-2018-04) clarified that ‘for a device to be considered possession, there needs to be a reliable means to confirm the possession through the generation or receipt of a dynamic validation element on the device’. This means that it is not always required that the device should perform cryptographically underpinned validity assertions using keys or cryptographic material stored in the device. In addition, paragraph 24 of the EBA Opinion on the elements of Strong Customer Authentication under PSD2 (EBA-Op-2019-06) clarified that ‘possession does not solely refer to physical possession but may refer to

	something that is not physical (such as an app)'. It follows from the above, that in the cases where the possession element is based on a device, the SCA process must reliably confirm that the specified device is in the physical possession of the Payment Service User (PSU). If the possession element is based on something not physical (e.g. a mobile app), in line with the requirements of Article 7 of the Delegated Regulation, the Payment Service Provider (PSP) should ensure that a unique connection is established between the possession element and the PSU. In both of the above cases, the PSP should in accordance with Article 7 of the Delegated Regulation mitigate the risk that the element is used by unauthorised third parties. Q&A 2018_4414 provides further clarity on the transmission of authentication codes or payment information under Article 5(2)(a) of the Delegated Regulation via a Short Message Service (SMS).
Link	https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4532

European Banking Authority, 21/03/2023
www.eba.europa.eu