Single Rulebook Q&A

Question ID	2020_5619
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	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	9
Date of submission	16/11/2020
Published as Final Q&A	23/04/2021
Disclose name of institution / entity	No
Type of submitter	Other
Subject matter	Independence of the elements for SCA
Question	Can a Payment Service Provider (PSP) apply Strong customer authentication (SCA) using elements from the same category provided that the elements are independent (i.e. breach of one does not compromise reliability of the other elements)?
Background on the question	The EBA stated in its Opinion on the implementation of the RTS on strong customer authentication (SCA) and secure communication (EBA-

	Op-2018-04), June 2018, that the two authentication elements (for SCA) need to belong to two different categories (i.e., knowledge, possession or inherence). The EBA RTS does not require authentication elements to belong to separate categories but impose a requirement on PSPs to adopt measures to ensure that the elements are independent. The view that authentication elements should come from separate categories can restrict innovation, development, and adoption of new elements which, although they fall into the same category, meet all the security and independence requirements under the EBA RTS. The rationale for using authentication elements from separate categories is that adopting elements from different categories reduces the risk if one of the channels used by the Payment Service User (PSU) is compromised, enabling the PSP to fulfil the requirements of Article 9 of the RTS. However, using elements from separate categories is not the only way of ensuring that the elements are independent. In fact, there are elements that although they may belong to the same category, are independent. Additionally, PSPs can implement security measures to ensure that breach of one element does not comprise reliability of the other element. As an example, technology on a mobile device can be used to securely read information on a card, passport or driver's license enabling a PSP to verify possession of the identity document or physical card. The combination of these elements (which are independent) can be used to provide a more secure way to verify consumers compared to other combinations of elements. Arguably, confirming physical possession of a bank card and a passport by reading the data contained in their chips is more secure than verification based on a password and SMS One Time Password (OTP). However, based on the EBA Opinion of June 2018, a verification based on a combination of an identity document and a physical card would not meet SCA as both elements are categorised as "possession". The EBA RTS requires that the use of the elements "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 other elements". It is possible to develop two authentication elements from the same category that are independent (i.e. breach of one does not compromise reliability of the other elements) and are more secure than other solutions that have been confirmed as meeting SCA requirements. We welcome clarification that SCA elements can be from the same category provided they are independent (breach of one does not compromise reliability of the other factor) as required under Article 9 of the RTS and use of the factors meets the requirements under Articles 6 - 9 of the RTS.
EBA answer	Article 4(30) of Directive 2015/2366/EU (PSD2) defines strong customer authentication as 'an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to

	protect the confidentiality of the authentication data'. In relation to this, Paragraph 33 of the EBA Opinion on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04) clarified that the two authentication elements 'need to belong to two different categories'. Article 9 of the Commission Delegated Regulation (EU) 2018/389 further specifies requirements on how to ensure independence of the authentication elements, including the adoption of security measures in the case where the authentication elements are used through a multi-purpose device. Therefore, payment service providers (PSPs) should apply strong customer authentication (SCA) by using at least two independent elements from different categories. However, PSD2 and the Delegated Regulation do not restrict PSPs from applying an additional element from the same categories to one of the elements already applied as an additional security measure.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5619

European Banking Authority, 03/05/2021
www.eba.europa.eu