Single Rulebook Q&A

Question ID	2020_5353
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	6, 7 and 8
Date of submission	06/07/2020
Published as Final Q&A	23/04/2021
Disclose name of institution / entity	Yes
Name of institution / submitter	Derek Dempsey
Country of incorporation / residence	UK
Type of submitter	Consultancy firm
Subject matter	On the requirements for 'inherence' in strong customer authentication (SCA)
Question	Do the elements required for ‘inherence’ in strong customer authentication (SCA) provide the complete authentication or can they form a part of an authentication decision with some non-biometric elements and still satisfy

	the inherence condition, for example, as one element of a user profile of several elements. For example, if the biometric, say keystroke dynamics, provides 50% of the decision and other characteristics (e.g. device data, location data) provide the other 50%, does this satisfy the requirement for inherence assuming the condition for 'very low probability of unauthorised access' is also satisfied and that another SCA condition, 'knowledge' or 'possession' is also satisfied? if so, is there a threshold, say 50%, below which it ceases to qualify as 'inherence'?
Background on the question	If a strong customer authentication (SCA) element is to count as 'inherence' it must involve physical properties, physiological characteristics or behavioural properties of the body or combination of these, based on paragraph 18 of the EBA Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06). I am concerned that keystroke dynamics is a very unproven approach to be catapulted into a 'preferred' approach for SCA for many merchants. Most vendors of this approach are clearly talking about behavioural profiling using other elements such as device ID, location data and user behaviours to supplement the behavioural biometric which is fine but suggests that few have confidence in keystroke dynamics alone as a 'strong' authentication factor. To me, this completely blurs the line with transactional risk analysis (TRA) which is excluded from being an SCA element (because a profile takes time to build up) and can only be used in exception conditions. So my concern is that a 'weak' or untested certainly, authentication element is being permitted for SCA by this blurring of boundary and that the fraudsters will be quick to take advantage and the purpose of the SCA regulation undermined. If it is made clear the 'inherence' means 'inherence' and only 'inherence' then clarity is restored. Behavioural elements can be used to enhance accuracy and security but the inherence element alone needs to be sufficient.
EBA answer	Article 4(30) of Directive 2015/2366/EU (PSD2) defines strong customer authentication (SCA) 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’. Paragraph 33 of the EBA Opinion on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04) clarified that ‘the two factors [the two elements] need to belong to two different categories’. Article 8(1) of the Commission Delegated Regulation (EU) 2018/389 states, ’Payment service providers (PSPs) shall 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 payment service providers shall ensure that those access devices and software have a very low probability of an unauthorised party being authenticated as the payer'. Paragraph 18 of the EBA Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06) states that 'inherence, which includes biological and behavioral biometrics, relates to physical properties of body parts, physiological characteristics and behavioral processes created by the body, and any combination of these'. Paragraph 19 of the EBA Opinion (EBA-Op-2019-06) states that 'Inherence may include retina and iris scanning, fingerprint scanning, vein recognition, face and hand geometry (identifying the shape of the user's face/hand), voice recognition, keystroke dynamics (identifying a user by the way they type and swipe, sometimes referred to as typing and swiping patterns), the angle at which the Payment Service User (PSU) holds the device and the PSU's heart rate (uniquely identifying the PSU), provided that the implemented approaches provide a 'very low probability of an unauthorised party being authenticated as the payer', in accordance with Article 8 of the RTS on SCA and CSC'. Accordingly, the inherence element is related to something the user is or defined by the user's physiological behaviour and should by itself meet the requirements of Article 8 of the Delegated Regulation, including that the access devices and software have a very low probability of an unauthorised party being authenticated as the payer. The use of additional data elements, such as location or browser data, are not part of the SCA but may be used by the PSP as an additional security measure, in particular for the purposes of Article 2 of the Delegated Regulation, which explicitly requires PSPs to adopt transaction monitoring mechanisms 'that enable them to detect unauthorised or fraudulent payment transactions for the purpose of the implementation of the security measures'. Finally, the location or browser data can also be used separately for the purpose of the exemption from the SCA under Article 18 on transaction risk analysis.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5353