Single Rulebook Q&A

Question ID	2020_5626
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	24
Paragraph	2
Subparagraph	b
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	98
Date of submission	18/11/2020
Published as Final Q&A	24/09/2021
Disclose name of institution / entity	Yes
Name of institution / submitter	ING bank
Country of incorporation / residence	Netherlands
Type of submitter	Credit institution
Subject matter	Association with the payment service user by means of a remote channel
Question	Is it sufficient to use a company level knowledge element, in combination with a peronal posession element to associate a user of a business application with personalised security credentials such as authentication

	software or a knowledge element?
Background on the question	When associating a user with personalised security credentials through a remote channel, it is required by the RTS on strong customer authentication and secure communication, Article 24.2.b, that strong customer authentication (SCA) is performed. In a business application, the association of the identity of the user is performed in 2 steps. 1) A possession element is associated with the user in a secure environments under the payment service provider's responsibility and than securely delivered to the customer. 2) After delivery the possession element the possession element is used in combination with a company level secret to activate the possession element and create a new personalized knowledge element. After this association and activation process the user can access the business application on behalf of the company using the possession element and the personalized knowledge element.
EBA answer	Article 4(29) of Directive 2015/2366/EU (PSD2) defines authentication as 'a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials'. Article 4(30) of PSD2, in turn, defines the authentication element knowledge as 'something only the user knows'. Article 4(31) of PSD2 defines personalised security credentials (PSC) as 'personalised features provided by the payment service provider to a payment service user for the purposes of authentication'. Article 6(1) of the Commission Delegated Regulation (EU) 2018/389, in turn, requires payment service providers (PSPs) to 'adopt measures to mitigate the risk that the elements of strong customer authentication categorised as knowledge are uncovered by, or disclosed to, unauthorised parties'. Article 24(2)(b) of the Delegated Regulation prescribes that 'the association by means of a remote channel of the payment service user's identity with the personalised security credentials and with authentication devices or software is performed using strong customer authentication'. Accordingly, PSPs cannot use company level knowledge as a valid SCA element to associate the payment service user (PSU) with the PSC since it will not allow the PSP to verify unequivocally the identity of the PSU and to mitigate the risk that the knowledge element is disclosed to unauthorised parties. The provision of the knowledge element should be carried out based on procedures set out by the PSP.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5626