Single Rulebook Q&A

Question ID	2018_4338
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	98
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	13
Date of submission	24/10/2018
Published as Final Q&A	09/04/2021
Disclose name of institution / entity	No
Type of submitter	Credit institution
Subject matter	Trusted Beneficiaries
Question	Article 13 of the RTS on strong customer authentication (SCA) and secure communication does not seem to restrict the use of trusted beneficiaries beside the fact that the payee must be in the list of trusted beneficiaries when initiating the payment transaction. Is it correct to conclude from this that the usage of trusted beneficiaries is not further restricted and can, therefore, also be implemented as a generic beneficiary approval step prior to every initiation of a payment transaction?
Background on the question	Article 97.2 of the PSD2 Directive and Article 5 of the RTS on strong customer authentication and secure communication require payment service providers to apply SCA that includes elements which dynamically link the transaction to a specific amount and a specific payee for the initiation of electronic payment transactions. Article 13 of the RTS allows payment service providers to not apply SCA where the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer. SCA is to be applied where a payer creates or amends a list of trusted beneficiaries.The requirement for applying SCA aims at increasing security whilst reducing the risk of fraud. Applying SCA

	with dynamic linking to the payee and the amount when initiating a payment transaction aims at providing additional security beyond SCA without dynamic linking. However, the concept of trusted beneficiaries does not hinder an attacker adopting whitelisting with SCA (without any linking) for approving a new payee before initiating a fake payment. There appears to be no legitimate security rationale to limit a Payment Services User (PSU) beyond what an attacker is effectively limited to. The risk of circumvention by an attacker can consistently be mitigated e.g. by implementing, beyond current RTS requirements, SCA with dynamic linking to the payee whenever adding a new payee to the list of trusted beneficiaries.
EBA answer	Under Article 13(2) of the Commission Delegated Regulation (EU) 2018/389, payment service providers "shall be allowed not to apply strong customer authentication where the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer". Article 13 of the Delegated Regulation does not restrict the use of the trusted beneficiary list by payment service providers for other purposes such as the introduction of an option for the payer to add a new payee to the general trusted beneficiary list as an additional step in the approval process prior to every initiation of a new payment transaction. However, in accordance with Article 13(1) of the Delegated Regulation, adding the payee to the general trusted beneficiary list requires the application of strong customer authentication, including when done prior to the initiation of the payment transaction. The above is without prejudice to the clarifications provided in Q&A 2018_4076.
Link	https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4338