Table of Contents

Question ID: 2018_4141

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
1

Subparagraph

COM Delegated or Implementing Acts/RTS/ITS/GLs
Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication

Article/Paragraph
4

Date of submission
18/07/2018 20:19

Published as Final Q&A
24/05/2019 11:37

Type of submitter
Credit institution

Subject matter
Authentication code

Question

Is it allowed to use the (authenticated) session that a user has (after logging in (with or without SCA)) as 1 of the authentication factor when performing SCA for a payment transaction?

For example: A customer logs in with its username & password (knowledge) + SMS One Time Password (possession). Once in his online banking environment he looks at his statements. Within that same session (that ends after 5 minutes inactivity) he makes a payment.

The question is if for authenticating the payment it is required to perform SCA again or if the authenticated session (based on the previous authentication) and a second SMS One Time Password (possession) that dynamically links the payment would suffice.

Background on the question

No additional security risk mitigation seen as a result of 're-asking' the first factor within a matter of minutes within the same session; however it will negatively influence the customer experience

EBA answer

Article 4 of the Commission Delegated Regulation 2018/389 states that "*where payment service providers apply strong customer authentication*", "*the authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code*".

In accordance with paragraph 36 of the EBA Opinion on the implementation of the RTS on Strong customer authentication (SCA) and common and secure communication (CSC) published in June 2018, "*SCA has to be applied to access to payment account information and to every payment initiation, including within a session in which SCA was performed to access the account data, unless an exemption under the RTS applies* ".

The Commission Delegated Regulation does not prescribe a time limit for the provision of the two authentication elements necessary for SCA while within a session. When initiating a payment, SCA may therefore be performed when one of the elements used at the time the customer accessed its payment account online (including via a mobile app) is reused in compliance with Article 4, and the other element of SCA is carried out at the time the payment is initiated, provided that the dynamic linking element required under Article 97(2) PSD2 and detailed under Article 5 of the Delegated Regulation is present and linked to that latter element.

Link
EBA website link