# Single Rulebook Q&A

| | |
|---|---|
| **Question ID** | 2020_5366 |
| **Status** | Final Q&A |
| **Legal act** | Directive 2015/2366/EU (PSD2) |
| **Topic** | Other topics |
| **Article** | 97 |
| **Paragraph** | 2 |
| **Subparagraph** | - |
| **COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations** | Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication |
| **Article/Paragraph** | 5 |
| **Date of submission** | 14/07/2020 |
| **Published as Final Q&A** | 30/07/2021 |
| **Disclose name of institution / entity** | Yes |
| **Name of institution / submitter** | Multi-Stakeholder Group Mobile initiated SEPA (instant) credit transfers |
| **Country of incorporation / residence** | Belgium |
| **Type of submitter** | Industry association |
| **Subject matter** | Clarification on where the creation of the authentication code with dynamic linking for strong customer authentication (SCA) for electronic remote payment needs to be done |
| **Question** | Should the authentication code be computed and dynamically linked to the transaction data in a unique processing step prior or together with the |

| | |
|---|---|
| | payer’s authentication on the payer’s device, or can the authentication code be computed and dynamically linked in one or several subsequent steps in the payment process, possibly not on the payer’s device? |
| **Background on the question** | Article 5 of the RTS on strong customer authentication and secure communication states that the provisions for SCA with dynamic linking apply, in accordance with Article 97(2) of Directive (EU) 2015/2366, for electronic remote payment transactions. For mobile initiated credit transfers, there may be solutions whereby, at the payer’s authentication step, strong customer authentication (SCA), via their mobile device, the authentication code cannot be, in full or part, computed since the specific transaction amount and payee are not known yet. These elements allowing to compute the authentication code with dynamic linking as required for electronic remote payments are only available and managed at later steps in the payment process (e.g. by the payee’s mobile initiated SEPA credit transfers (MSCT) service provider or the payer’s MSCT servic |
| **EBA answer** | Article 97(1)(b) of Directive 2015/2366/EU (PSD2) requires payment service providers (PSPs) to apply strong customer authentication (SCA) when the payer initiates an electronic payment transaction. In the case of electronic remote payment transactions, Article 97(2) of PSD2 requires PSPs to apply SCA that includes elements, which dynamically link the transaction to a specific amount and a specific payee.<br><br>Article 5(1)(a) of Regulation (EU) 2018/389 specifies that ’where payment service providers apply strong customer authentication in accordance with Article 97(2) of PSD2, the payer shall be made aware of the amount of the payment transaction and of the payee’. Further, Article 5(1)(b) and (c) of the Delegated Regulation require respectively that ’the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction’ and that ’the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer’.<br><br>The Delegated Regulation does not specify the technical solution as to how the dynamic linking requirements could be implemented. Therefore, it is not required that the authentication code is computed on and dynamically linked to the payer’s device.<br><br>In relation to the above, provided that the above-mentioned legal requirements are being met, the authentication code could be generated and dynamically linked to the amount of the payment transaction and the payee at any stage before the final authorisation of the payment transaction by the payment services user. |

| | |
|---|---|
| | However, it should be noted that in accordance with Article 5(2) of the Delegated Regulation, PSPs shall adopt security measures which ensure the confidentiality, authenticity and integrity of the amount of the transaction and the payee, as well as on the information displayed to the payer, throughout all of the phases of the authentication, including the generation, transmission and use of the authentication code.<br><br>Finally, Q&A 2020_5133 provides further information on the application of the dynamic linking requirements for remote electronic payment transactions where the exact transaction amount is not known at the moment when the payer gives consent to execute the payment transaction. |
| **Link** | https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5366 |

European Banking Authority, 27/11/2021
www.eba.europa.eu