# Single Rulebook Q&A

| | |
|---|---|
| **Question ID** | 2019_4910 |
| **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/Recommendations** | Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication |
| **Article/Paragraph** | 4 |
| **Date of submission** | 12/09/2019 |
| **Published as Final Q&A** | 25/09/2020 |
| **Disclose name of institution / entity** | No |
| **Type of submitter** | Credit institution |
| **Subject matter** | Authentication code |
| **Question** | Is an extra strong customer authentication (SCA) required, after logging in (with or without SCA) in the mobile application, to initiate the provisioning step to add the customers card to a third party wallet (e.g. Apple or Google pay)? |
| **Background on the question** | For example: A customer logs in to the mobile application with username & password (knowledge) + SMS One Time Password (possession). Once in his mobile banking environment he looks at his statements. Within that same session (that ends after 5 minutes inactivity) the customer selects the option to add the card to a third party wallet (in app provisioning). At this step is an extra SCA required? |
| **EBA answer** | Article 97(1) of Directive 2015/2366/EU (PSD2) states that payment service providers (PSPs) "shall apply strong customer authentication (SCA) where the payer:<br>(a) accesses its payment account online;<br>(b) initiates an electronic payment transaction; |

| | |
|---|---|
| | (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.”<br><br>Adding a payment card to a digital wallet is an action which may imply a risk of payment fraud or other abuses and thus would require the application of SCA. This means that, in the case described by the submitter, the payer would need to apply SCA for accessing its payment account via its mobile application, and apply a second SCA when adding the payment card to a digital wallet.<br><br>Q&A 2018_4141 clarified that, when initiating a payment while within the same session in which SCA was performed to access account data, one of the elements used at the time the customer accessed its payment account online (including via a mobile app) may be reused in compliance with Article 4 of the Commission Delegated Regulation (EU) 2018/389, provided that the other element of SCA is carried out at the time the payment is initiated and the dynamic linking element required under Article 97(2) PSD2 (for remote payment transactions) is present and linked to that latter element.<br><br>Further, the principle set out in Q&A 2018_4141 may be applied in the specific case described by the submitter. This means that one of the authentication elements used for accessing the payment account (via the mobile app) may be reused when adding the payment card to a digital wallet within the same session and within the same app, provided that the requirements of Articles 4, 6, 7, 8 and 9 of the Delegated Regulation are met. |
| **Link** | https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4910 |