Single Rulebook Q&A

Question ID	2022_6464
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	(c)
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	1
Date of submission	24/05/2022
Published as Final Q&A	31/01/2023
Disclose name of institution / entity	No
Type of submitter	Law firm
Subject matter	SCA for token replacement
Question	Is SCA required for the replacement of a tokenized card happening in the background without any 'action by the payer' under Article 97(1)(c) PSD2 in the following cases: 1. Expiry of the token and update of the token 2. Replacement of the card, and the new card has a different BIN/Account Range (e.g., for product graduation, such as standard to gold, or simple BIN management) and/or different functionalities 3. Technical and/or configuration changes to the issuer's BIN configuration (such as migrating from 6 to 8 digit BINs) In all these cases, the existing tokenized credentials have been initially associated with SCA to the user under Article 24(2)(b) RTS, and this is solely a technical replacement of the token. credentials have been initially associated with SCA to the user under Article 24(2)(b) RTS, and this is solely a technical replacement of the token.
Background on the	When cardholders register their cards in device-based wallet solutions, a

question	tokenized version of the card is created and uniquely associated with the user’s device (and can be used as a possession element for subsequent transactions). This tokenized version of the card can be used to carry out secure transactions without disclosing the actual details of the plastic card. All of the relevant and required SCA requirements are met when setting up the tokenized credentials. The EBA clarified that a tokenized card that is uniquely associated with a user/device may qualify as a valid ‘possession’ factor under the PSD2 RTS: “for approaches currently observed in the market, tokenised card payment solutions may constitute a possession element” (Q&A 4827; see also Table 2, page 7 of the EBA Opinion of June 2019). The EBA also clarified in the same answer that the initial association of the token with the user/device qualifies as an initial association of security credentials under Article 24(2)(b) RTS. In particular, this is an action that requires SCA under Article 97(1)(c) PSD2: “This requires, in accordance with Article 97(1)(c) of PSD2, the application of SCA at the time of the issuance of the token, which includes provisioning of the payment card details and the association of the token with the device under Article 24 of the Delegated Regulation.”. When the plastic card to which the token is linked expires or is replaced with another card, payers must activate their new cards with SCA before usage. Conversely, the token linked to the new card is automatically updated in the background without any ‘action by the payer’ under Article 97(1)(c) PSD2. This same automatic token replacement process also happens when a change has occurred on the card / issuer’s configuration, which in turn requires a technical replacement of the token. This happens, for example, when: A card issuer replaces the consumer’s plastic card with one in a different BIN/Account Range (e.g. product graduation from a standard to a gold product). An issuer performs an administrative or configuration task on their BIN, such as splitting it into smaller account ranges or migrating from 6 to 8 digit BINs. A technical fault occurs with the existing token, or with the token vault, or with the issuer’s system that may cause issues for the consumer. A token expires. We believe that SCA is not required for all the above-mentioned token replacement processes for the following reasons: The token replacement process is initiated by an action of the card issuer, and happens automatically in the background without any action by the cardholder. Hence, such process does not qualify as an action ‘by the payer’ within the meaning of Article 97(1)(c) PSD2, which requires SCA “where the payer […] carries out any action through a remote channel which may imply a risk of payment fraud or other abuses”. The updated token remains associated with the same user/device. Hence, there is no new association of security credentials with the user under Article 24(2)(b) RTS. The token replacement process is automatic and extremely secure (using existing and well-established provisioning mechanisms). It is performed in the same secure environment used for the initial provisioning, which prevents fraudsters from intercepting and stealing the new token. Hence, such process does not qualify as an action “which may imply a risk of payment fraud or other abuses” under Article 97(1)(c) PSD2. Payers expect that once

	their plastic cards expire or are replaced with new cards, they can continue shopping with their devices or online without having to manually update all the tokens in their devices. Whilst payers are aware of the expiry of their plastic card, the token’s expiry is generally not displayed to payers. The system is using the already established security and trust between the tokenization system and the consumer’s device. As neither the consumer nor the device has changed, there should be no need for new SCA. Payers should not need to be involved in the event that their card issuer has performed a maintenance task on their BIN (e.g., splitting the BIN), which has no other impact other than requiring a replacement set of tokenized credentials, since this is an administrative event. In this use case the consumer’s card is not changing, but due to the configuration changes a new set of tokenized credentials are required. This is, for example to ensure that any tokenized transactions use the correct parameters (associated with the newly split range) during processing. Requiring a new SCA for this process would have a very detrimental effect on the payment experience and cause disruptions for millions of consumers who rely on card-on-file and wallet solutions to conveniently pay for products and services. As issuers migrate from 6 to 8 digit BINs, the disruption caused by requiring SCA would cause a very detrimental effect to cardholders, and likely result in many calls and queries to issuers’ call centres. It is not reasonable to draw analogies between card replacement and token replacement in terms of security and risk. When a card is replaced, it is typically sent through the postal service, exposing it to the risk of loss, theft, or fraud. It is therefore expected that an issuer requires that the recipient performs some form of confirmation that the new card has arrived and has not been tampered with in transit. Tokens, however, only exist on devices that have been previously authenticated, and the relationship and secured channels between the token service provided and the device does not change as a result of updating/replacing the token credentials. Whilst replacing expiring tokens is performed automatically, Token Service Providers only replace tokenized credentials on instruction of the corresponding issuer (e.g., through an update to the card details, or a BIN split). Communications with the issuer is also through secure channels, and uses well established security mechanisms. This ensures that not only are tokens only updated through issuer instruction, but the issuer is also aware that the update has taken place.
Final answer	Article 97(1)(c) of Directive 2015/2366/EU (PSD2) requires payment service providers (PSPs) to apply strong customer authentication (SCA) ‘where the payer carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.’ Article 24(1) of the Delegated Regulation further prescribes that ‘payment service providers shall ensure that only the payment service user (PSU) is associated, in a secure manner, with the personalised security credentials, the authentication devices and the software’.

	Q&A 4827 clarified that ‘SCA should be applied at the time of the issuance of the token, which includes provisioning of the payment card details and the association of the token with the device under Article 24 of the Delegated Regulation.’ Accordingly, the issuance of a new token, replacing a previously existing one, and binding it to a device/user would require the application of SCA.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2022_6464

European Banking Authority, 31/01/2023
www.eba.europa.eu