Single Rulebook Q&A

Question ID	2020_5622
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	70
Paragraph	-
Subparagraph	-
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	16/11/2020
Published as Final Q&A	31/01/2023
Disclose name of institution / entity	No
Type of submitter	Other
Subject matter	Application of SCA to issuing a payment instrument and tokenisation
Question	Is strong customer authentication (SCA) required when a Payment Service Provider (PSP) issues a payment instrument or creates a token?
Background on the question	Payment tokenisation enhances the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorised or fraudulent use of primary account numbers (PANs) or IBANs. Payment tokenisation achieves this by substituting PANs or IBANs with payment tokens that differ significantly in terms of the ability to control or restrict usage to a particular transaction environment, device or other domain. Prior to issuance of a new token to a Payment Service User (PSU), a PSP is required to verify that that cardholder is the rightful user of the PAN / IBAN, and bind the payment token to the underlying PAN / IBAN and the PSU. Following verification of the cardholder, the PSP issues a new token linked to the cardholder and the respective PAN / IBAN, creating a new payment instrument that can be used by the PSU to make tokenised transactions. Article 70 of PSD2 sets out the obligations of a PSP in relation to payment instruments, including ensuring that personalised security credentials are not accessible by third parties, refraining from sending

	unsolicited payment instruments, and enabling blocking / unblocking of the payment instrument. The PSP bears the risk of sending a payment instrument or any other personalised security credentials relating to it to the PSU. Article 4(45) of PSD defines the “issuing of payment instruments” as “a payment service by a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer’s payment transactions”. The issuance of a payment token to a PSU falls under this definition of “issuing of payment instruments” in (Article 4(45) of PSD) as it involves a PSP providing a payer with a payment instrument to initiate and process payment transactions. The obligations of the PSP regarding issuance of the payment instrument (i.e., the token) are expressly and definitively set out in Article 70 of PSD rendering Article 97 inapplicable to issuance of payment tokens. It is noteworthy that Article 97 of PSD2 relates to actions undertaken by a payer in the course of making a payment transaction, i.e., accessing an account, initiating a payment or undertaking an action that implies risk of payment fraud or other abuse. The creation of a payment instrument is not undertaken during a payment transaction, but involves a PSP issuing a new payment instrument to the payer for subsequent use. The PSP remains under an obligation to correctly verify the PSU prior to issuing the payment instrument following the rules set out in Article 70 of PSD2 and not Article 97 of PSD2 or Articles 6-9 of the EBA RTS which apply to payment transactions. PSPs are required to follow the requirements set out in Article 70 of PSD2 in relation to issuing a payment instrument, including ensuring that the personalised security credentials are not accessible to parties other than the payment service user, refraining from sending unsolicited payment instruments, ensuring appropriate means are available to block the payment instrument following loss, theft, misappropriation or unauthorised use. PSPs continue to bear the risk, by virtue of Article 70(2) of PSD2, of sending a payment instrument or any personalised security credentials to the PSU. The requirements under Article 70 of PSD2 provide adequate protection to PSUs in relation to issuance of payment instruments (such as tokens).
Final answer	The creation of a token for the use of an issued and existing payment instrument encompasses various obligations and requirements laid out, amongst others, in article 70 and 97 of Directive (EU) 2015/2366 (PSD2). More related requirements can also be found in the Delegated Regulation 2018/389 (RTS SCA). The obligations for the issuing of payment instruments are in general laid out in article 70 PSD2, which includes that the payment services provider (PSP) issuing the payment instrument has to safeguard the personal security credentials, should not send unsolicited payment instruments and should enable payment service users (PSUs) to request a payment instrument to be unblocked. Beyond that, PSPs are obliged to apply SCA where required by article 97

	PSD2 and where no exclusion according to the RTS SCA is relevant. PSPs are, according to article 97(1) PSD2, required to apply SCA when the payer is accessing a payment account online, when initiating an online payment transaction and when carrying out any action through a remote channel, which may imply the risk of payment fraud or other abuses. Article 97(3) PSD2 furthermore requires the PSPs to have in place, when the payer is performing any of the actions listed under article 97(1) PSD2, adequate security measures to protect the confidentially and integrity of PSU´s personalised security credentials. Creating a token, based on the submitter´s description, includes the verification by the PSP that the PSU (e.g. cardholder) is the rightful user of the payment card details and the device, and the association of the token with the device under article 24 of the RTS SCA. A created token, representing a pre-existing and -issued payment instrument, can then be used to initiate payment transactions amounting to a digitised version of a payment instrument. In the process described, the creation of a token is done via a remote channel and with the participation of the payer thus requiring the application of SCA in accordance with article 97(1)(c) of PSD2 by the PSP of the PSU as these processes may imply the risk of payment fraud or other abuses.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5622

European Banking Authority, 29/05/2023
www.eba.europa.eu