Single Rulebook Q&A

Question ID	2020_5477
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Security measures for operational and security risks
Article	Article 66
Paragraph	3
Subparagraph	(f),(g)
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	Article 35, paragraph 1
Date of submission	04/09/2020
Published as Final Q&A	24/09/2021
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 level of protection required for the processing of the IBAN outside the inter-PSP environment
Question	Can the IBAN of the payer or payee be handled in cleartext outside the inter Payment Service Provider (PSP) environment? For instance could a payer's IBAN be contained in cleartext in a payer-presented QR-code provided by the

	payer's device to the merchant's point of interaction for the initiation of an (instant) credit transfer? Or could a merchant's IBAN be contained in cleartext in a merchant-presented QR-code at the merchant's point of interaction to be read by the payer's device for the initiation of an (instant) credit transfer?
Background on the question	Article 4 (32), PSD2, provides that for the activities of Payment Initiation Service Providers (PISPs), i) the name of the account owner and ii) the account number (the IBAN) do not constitute sensitive payment data. In line with the clarifications given under the EBA Q&A 2018_4081, if the transaction is initiated in accordance with the rules of Article 36 (1), RTS and provided that the PISP complies with Article 66 (3), PSD2, it seems possible that the IBAN could be used/displayed in cleartext in an Application Programming Interface (API) environment. It is however unclear whether the same would apply in case of presentation of the IBAN in cleartext as part of the payer-presented-QR provided by the payer's device to the merchant at point of interaction (POI) (or vice-versa) for the initiation of an (instant). In particular, from a security perspective, it is unclear whether in a POI context the IBAN could be shown to all parties without tokenisation and still comply with Article 35 (1), RTS on security of communication.
EBA answer	Article 4(31) of Directive 2015/2366/EU (PSD2) defines personalised security credentials (PSC) as 'personalised features provided by the payment service provider to a payment service user for the purposes of authentication'. Accordingly, since the IBAN is not an element used for the purpose of authentication, it cannot be considered as a PSC. Article 4(32) of PSD2 defines sensitive payment data as 'data, including personalised security credentials which can be used to carry out fraud. The article further clarifies that 'for the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data'. Accordingly, the IBAN of the payer does not constitute sensitive payment data for the activities of payment initiation service providers. In relation to the above, in a transaction initiated at the point-of-interaction (POI) by using a QR code presented by either the payer or the payee (merchant), the IBAN can be included in free text. However, since its disclosure may be used to carry out fraud, it will be for payment service providers to assess the risks arising from transmitting the IBAN in free text between the device of the payer and the POI and from

	storing it, if applicable. Subsequently, PSPs should decide whether it is necessary to implement corresponding security measures to mitigate these risks.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5477

European Banking Authority, 22/10/2021
www.eba.europa.eu