Single Rulebook Q&A

Question ID	2020_5476
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	-
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 5
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 the qualification and protection requirements of a CustomerID when included in a payer-presented QR-code for the initiation of (instant) credit transfers at the point of interaction (POI)
Question	Is the CustomerID (i.e. ID issued by an Account Servicing Payment Service Providers (ASPSP) to its Payment Services User (PSU) for accessing the on-

	line banking system and usually required by PSD2 Application Programming Interfaces (APIs) to identify the PSU) to be qualified as “personalised security credentials of the PSU” within the meaning and for the purposes of Article 66 (3) b), PSD2, and Article 35 (5), RTS, and therefore be treated as “sensitive payment data” within the definition of Article 4 (32), PSD2? Accordingly, can said CustomerID be included in cleartext in the payer-presented QR-code for the initiation of (instant) credit transfers at the point of interaction (e.g. POS, vending machine) without any protection during the QR-code life-cycle, including the generation of the QR-code, storage of the QR-code on the payer’s device, transmission from the payer device to the payee’s point of interaction and in the payee’s (e.g. merchant) point of interaction?
Background on the question	Payer-presented QR-codes could be used to initiate (instant) credit transfers at the point of interaction. To enable the involvement of a PISP and their usage of a PSD2 API to initiate the (instant) credit transfer, the QR-code should contain the CustomerID in cleartext (i.e. ID issued by an ASPSP to its PSU payer for accessing the on-line banking system). It is however not clear whether said CustomerID is to be qualified as “personalised security credentials” within the meaning and for the purposes of Article 66 (3) b), PSD2 and Article 35 (5), RTS, and should therefore be treated as “sensitive payment data” as defined by Article 4 (32), PSD2. If so, would the inclusion of the CustomerID in cleartext as part of the payer-presented-QR at POI conflict with: - the provisions of Article 66 (3) b), providing that a PISP “shall ensure that the personalised security credentials of the PSU are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the PISP through safe and efficient channels.” - the provisions of Article 35 (5), RTS, which mandates that ASPSPs and PISPs shall ensure that where they communicate personalised security credentials and authentication codes, “these are not readable, directly or indirectly, by any staff at any time”?
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’. Guideline 3.4.1 of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) (which repealed the Guidelines on security measures for operational and security risks (EBA/GL/2017/17) as of 30 June 2020) specifies that the information security policy ‘should ensure the confidentiality, integrity and availability of … sensitive data whether at rest, in transit or in use’. Guideline 3.4.4 further specifies that financial institutions, including payment service providers, should implement procedures to ‘prevent the occurrence of security issues in ICT systems and ICT services and should minimise their impact on ICT service delivery’ and that the procedures should include inter alia measures ensuring encryption

	of data at rest and in transit. Accordingly, the Customer ID facilitates the identification of the Payment Services User (PSU) for the purpose of authentication but is not in itself a valid Strong Customer Authentication (SCA) element . Therefore, it cannot be considered as a PSC. However, Customer ID is not available to third parties other than the payment service user and the payment service provider, and its disclosure can be used to carry out fraud. Therefore, taking also into account the above provisions of the GL on ICT and security risk management, the Customer ID cannot be included in a cleartext in a payer-presented QR-code for the initiation of credit transfers at the point of interaction without any security measures (e.g. encryption, tokenisation, transport layer security) ensuring its confidentiality during the QR-code life-cycle.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5476

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