Single Rulebook Q&A

Question ID	2018_4077
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	-
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	22
Date of submission	04/07/2018
Published as Final Q&A	12/03/2021
Disclose name of institution / entity	Yes
Name of institution / submitter	Banque de France
Country of incorporation / residence	FRANCE
Type of submitter	Competent authority
Subject matter	On the use and storage of Personalised Security Credentials (PSC)
Question	Do third party providers (TPPs) have the right to ask for payment service users (PSUs)' Personalised Security Credentials (PSC)? Do TPPs have the right to store PSUs' PSC ?
Background on the question	Three articles (Article 22.2 of the RTS, Articles 66 and 67 of PSD2) define obligations related to the storage and use of PSCs by TPPs, i.e.:Article 22.2 of the RTS :« 2.For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met: […] (b) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plain text; […] »Article 66« Rules on access to payment account in the case of payment initiation services (PIS)[…]3. The payment

	initiation service provider shall:[…](e) not store sensitive payment data of the payment service user;(f) not request from the payment service user any data other than those necessary to provide the payment initiation service;[…]Article 67« Rules on access to and use of payment account information in the case of account information services[…]2. The account information service provider shall:[…](e) not request sensitive payment data linked to the payment accounts;(f) not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.[…]We understand from the following articles that:PIS will be transmitting encrypted authentication codes/PSC of the user to the Account Servicing Payment Service Provider (ASPSP), i.e. they will be accessible to PIS, but not read by the PIS. Accordingly, the PIS will also not be able to use the transmitted authentication code/PSC for any other purposes than the payment initiation of a concrete payment transaction, and will therefore not be able to store the PSCs at all (even if encrypted).Account Information Service (AIS) will get the encrypted/tokenized PSC/authentication codes that will be transmitted through safe and efficient channels to ASPSP; however no reading of PSC is needed by the AIS in order to perform the necessary services.
EBA answer	Payment initiation service providers (PISPs) have the right to ask for payment service users (PSUs)' personalised security credentials (PSCs) only if this is necessary to provide the payment initiation service (Article 66(3)(f) Directive 2015/2366/EU (PSD2)) and subject to the explicit consent of the PSU. In accordance with Article 66(3)(e) PSD2, PISPs have no right to store the PSU's PSC. On the basis of Article 67(2)(f) PSD2, account information service providers (AISPs) may use and store the PSU's PSCs only if this is necessary to perform the account information service explicitly requested by the PSU and only if transmitted and stored in the encrypted form and without reading them in accordance with Article 22 of the Commission Delegated Regulation (EU) 2018/389. This storage should not be used to circumvent the application of strong customer authentication as per Article 97 PSD2 and Article 10 of the Commission Delegated Regulation (EU) 2018/389 (rule for 90 day-re-authentication). Furthermore, the provision in Article 67(2)(b) obliges AISPs not to make the PSC accessible to other parties. The PSU's PSCs must be secured at all times, according to the rules laid down in PSD2 and the Commission Delegated Regulation (EU) 2018/389. Disclaimer: The answers clarify provisions already contained in the applicable legislation. They do not extend in any way the rights and obligations deriving

	from such legislation nor do they introduce any additional requirements for the concerned operators and competent authorities. The answers are merely intended to assist natural or legal persons, including competent authorities and Union institutions and bodies in clarifying the application or implementation of the relevant legal provisions. Only the Court of Justice of the European Union is competent to authoritatively interpret Union law. The views expressed in the internal Commission Decision cannot prejudge the position that the European Commission might take before the Union and national courts.
Link	https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4077

European Banking Authority, 29/01/2022
www.eba.europa.eu