Table of Contents

Question ID: 2018_4055

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
Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication

Article/Paragraph
22

Date of submission
28/06/2018 15:48

Published as Final Q&A
19/07/2019 13:09

Type of submitter
Other

Subject matter
Confidentiality of offline PIN

Question

Should the PIN transmitted offline from a terminal to an Europay, MasterCard and Visa (EMV) card always be enciphered?

Background on the question

The EMV specification allows PIN validation to be performed offline between the card and the terminal. The PIN is stored securely on the chip itself. When the cardholder enters the PIN on the terminal, the PIN is transmitted to the EMV card for validation. The transmission of the PIN from the terminal to the card may be enciphered or in plain text.

The EBA has already stated that "in an EMV chip offline transaction, either the PIN is verified offline (i.e. just between the chip and the terminal) or the transaction itself is authorised offline - usually within certain value limits. If the PIN is given, the offline transaction could be SCA compliant." (Question 273 of Feedback Table annexed to the final draft RTS of February 23, 2017.)

The question is whether a PIN may be transmitted from the terminal to the card in plain text or should always be enciphered.

Our view is that a PIN may be transmitted from the terminal to the card in plain text under certain conditions. The conditions are that the PIN is sufficiently long (e.g., 4 or 5 digits) and complies with the RTS entropy requirements (e.g., 0000 is not allowed) and that the cardholder enters the PIN via a PCI-compliant PIN Entry Device. PCI-compliant PIN Entry Devices allow for a secure transmission of the PIN even if the PIN is transmitted in plaintext. This is because, according to the PCI Security Standards, PIN Entry Devices must comply with several physical and logical security requirements.

EBA answer

A PIN that is transmitted and verified offline constitutes a personalised security credential (PSC) and therefore is subject to the requirements of Chapter IV of the Commission Delegated Regulation (EU)

2018/389. In particular, Article 22(1) of the Delegated Regulation states that payment service providers (PSPs) "shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user". Article 22(4) of the Delegated Regulation, in turn, requires that PSPs "shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter II take place in secure environments in accordance with strong and widely recognised industry standards."

In addition, Article 6(1) of the Delegated Regulation states that "payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as knowledge are uncovered by, or disclosed to, unauthorized parties." Article 6(2) of the Delegated Regulation further states that "the use by the payer of those elements shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties."

In relation to the above, the transmission and verification of the PIN offline would need to be carried out in a secure environment ensuring confidentiality and integrity of the Personalised security credential (PSC), which may, but is not necessarily required to, include encryption. Nevertheless, in the case where a PSP does not use encryption, said PSP should assess the risks arising from transmitting the PIN in plain text between the terminal and the card, and if needed, implement corresponding security measures to mitigate these risks.

Link
EBA website link