Question ID

2025_7376

Legal act

Directive 2015/2366/EU (PSD2)

Topic

Strong customer authentication and common and secure communication (incl. access)

Article

97

Paragraph

1

COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations

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

Article/Paragraph

35

Name of institution / submitter

Central Bank of Hungary

Country of incorporation / residence

Hungary

Type of submitter

Competent authority

Subject matter

the use of strong and widely recognized encryption techniques

Question

All strong and widely recognized encryption techniques (e.g. RSA and ECC) currently available on the market must be provided by the account servicing payment service providers or only that encryption technique which is indicated in the documentation of

the technical specification of the API in accordance with Article 30(3) of the RTS on SCA & CSC shall be provided?

Background on the question

Pursuant to Article 35(1) of RTS on SCA & CSC account servicing payment service providers, payment service providers (hereinafter: ASPSPs) issuing card-based payment instruments, account information service providers and payment initiation service providers shall ensure that, when exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.

However, in this context, the SCAr does not regulate whether payment service providers are obliged to use (adopt) only one or more of the strong and widely recognised encryption techniques (e.g. currently RSA and ECC), as indicated in the technical specification documentation of the access interface in accordance with the second subparagraph of Article 30(3) of the the RTS on SCA & CSC.

Some ASPSPs have decided not to provide all strong and widely recognized encryption techniques only RSA and this caused refused API call connections because of the use of an ECC algorithm certificate.

Submission date

10/03/2025

Final publishing date

03/10/2025

Final answer

Article 35(1) of the Commission Delegated Regulation (EU) 2018/389 (RTS SCA&CSC) prescribes that 'account servicing payment service providers (ASPSP), payment service providers issuing card-based payment instruments (CBPII), account information service providers (AISP) and payment initiation service providers (PISP) shall ensure that, when exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.'

In that regard, any strong and widely recognised encryption techniques can be used to safeguard the confidentiality and the integrity for the exchange of data.

Accordingly, an ASPSP that has indicated a particular encryption technique in documentation of the technical specification of the application programming interface (API) that meets the requirements of Article 35(1), would not be required to provide all strong and widely recognised encryption techniques.

Status

Final Q&A

Answer prepared by

Answer prepared by the EBA.