Question ID

2024_7286

Legal act

Directive 2015/2366/EU (PSD2)

Topic

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

Article

4 and 98

Paragraph

article 4.30 and article 98.1.a

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

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

Article/Paragraph

article 6 and article 9

Type of submitter

Competent authority

Subject matter

Knowledge element of SCA.

Question

Can an API key be considered as a Knowledge element of SCA?

Background on the question

SCA means an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent.

The financial entity has chosen to use for SCA the combination of the possession element and the knowledge element.

The financial entity has only corporate customers.

For the possession element the customer has to set-up a HSM in its own environment, generate a key-pair, store the private key in the HSM and send via a secure connection the public key to the financial entity.

For the knowledge key, the customer has to log in to the financial entity portal, based on an userid and an OTP(One Time Password, received from the financial entity), and create what the financial entity calls an API-key. The API key is created by the financial entity and during the creation the key is shown in plain text for a very short moment. After the creation the API Key cannot be viewed in plain text again. The customer must securely store the API key. The financial entity suggests to store the API Key in for example a file, database, key vault or HSM. This could also be the same HSM as used by the customer for the private key of the possession element.

The hash of the API key is stored by the financial entity. The hash is used by the financial entity to valid the use of the knowledge element at the authorisation of the transaction done by the customer.

For the initiation of transactions the customer has to sign with his private key and to copy the API key as knowledge element in the financial entity portal.

Submission date

18/12/2024

Final publishing date

29/08/2025

Final answer

According to Article 4, point (30) of Directive (EU) 2015/2366 (PSD2), ‘strong customer authentication’ (SCA) means “an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data”.

An API key may constitute a valid SCA knowledge element, provided that the Payment Service Provider (PSP) complies with all applicable requirements under Commission Delegated Regulation (EU) 2018/389 (the RTS on SCA). This includes:

- The obligation under Article 6(1) to adopt measures to mitigate the risk that elements categorised as knowledge are uncovered by or disclosed to unauthorised parties.
- The requirement under Article 9 to ensure the independence of the SCA elements.
- The obligation under Article 24(2)(b) to ensure that the association, by means of a remote channel, of the Payment Service User (PSU)'s identity with the personalised security credentials and with authentication devices or software is performed using strong customer authentication.

While memorisation is not explicitly required, an SCA knowledge element should be known only to the user and not accessible to unauthorised parties or retrievable by the system itself.

Additionally, the API key, as an SCA factor, should be associated with the PSU in accordance with Article 24(2)(b) of the Delegated Regulation. In the case described by the submitter, the association with the PSU does not appear to meet the requirements of Article 24(2)(b), as only one valid SCA factor is used (possession via a one-time password). As clarified in the EBA Opinion (EBA-Op-2018-04), a user ID does not constitute a valid knowledge element. Based on the information provided by the submitter, it cannot be concluded whether the requirements of Articles 6(1) and 9 of the Delegated Regulation are met.

In conclusion, whether an API key qualifies as a knowledge element depends on its implementation.

Status

Final Q&A

Answer prepared by

Answer prepared by the EBA.