Public Consultation

European Payments Council

European Payments Council AISBL,
Cours Saint-Michel 30 B-1040 Brussels
T +32 2 733 35 33
Enterprise N°0873.268.927
secretariat@epc-cep.eu

EPC 276-22
Version 1.0
Date issued: 16 December 2022

Public

Approved

Public consultation on the extension of SCA related sections in version 1.0 of the SPAA scheme rulebook

1 Background and objectives

The European Payments Council (EPC) is launching a public consultation on the extension of sections in version 1.0 of the SEPA Payment Account Access (SPAA) scheme rulebook (EPC012-22 version 1.0) about the usage of Strong Customer Authentication (SCA).

In response to the feedback received on the list of 'eligible SCA approaches' from the public consultation on the draft Rulebook that ended on 12 September 2022 (where the market was invited to share its suggestions), the SPAA Multi Stakeholder Group (MSG) has drafted the below further clarification to facilitate SCA usage under the scheme.

The outcome of this new, focused public consultation will be integrated in a revised version of the first SPAA scheme rulebook.

The public consultation will run for a 90-calendar day period from 16 December 2022 up to and including 15 March 2023 (midnight Brussels time).

The SPAA scheme, which is created in line with the requirements defined in the June 2021 report of the Euro Retail Payments Board (ERPB) Working Group on a SEPA Application Programming Interface (API) Access scheme, covers the set of rules, practices and standards that will allow the exchange of payment accounts related data and facilitates the initiation of payment transactions in the context of 'value-added' ('premium') services provided by asset holders (i.e. Account-Servicing Payment Service Providers (ASPSP)) to asset brokers (e.g. Third Party Providers (TPP)).

The aim of the scheme is to drive 'open payments' in a way that unlocks and creates value whilst allowing for a fair distribution of value and risk between scheme participants.

The scheme covers messaging functionalities. It is not about a payment means or a payment instrument, but it offers a way to transport information in relation to payment accounts and transactions.

It is envisaged that the scheme will evolve further over time to support more elaborated functionalities, in line with market demand.

The publication of the formal first version of the scheme took place on 30 November 2022. The SPAA scheme itself will enter into force in November 2023.

2 The extension of SCA sections in version 1.0 the SPAA scheme rulebook

Note: The text highlighted in grey is already included in version 1.0 of the SPAA scheme rulebook (EPC 012-22[1]) and it is only provided here to help the reader better understand how these extended sections will be incorporated in the rulebook. The highlighted text should hence not be reviewed as part of this public consultation.

2.2.3 SCA exemptions and delegations implemented

This is a service that helps the Asset Broker identify the SCA exemptions and delegations supported by a specific Asset Holder.

In case one or more of the supported exemptions and delegations are not available for a concrete Asset User or Payer, these would not be communicated prior to the transaction requiring the SCA. The Asset Holder should however apply all the available SCA exemptions unless the Payer had opted out.

This service is available to Asset Brokers via a directory service (to be determined who provides the service). The directory could be updated via a discovery API provided by the Asset Holder. Further details are provided as part of the directory service definition.

The SCA exemptions are defined in the RTS on SCA and include:

- Credit transfers between accounts held by the same natural or legal person.
- Low-value transactions.
- Contactless payments at point of sale.
- Etc.

2.2.3.1 Business Rules

As mentioned in the final report of the ERPB Working Group on a SEPA Application Programming Interface (API) Access Scheme, the SPAA Scheme strives for a maximum use of the SCA exemptions foreseen in the law in as much as this may constitute a material competitive advantage of such a scheme-based solution offered by Asset Brokers.

SCA-obliged parties, e.g., Asset Holders not using SCA delegation, who participate in the Scheme have to consistently implement a predictability mechanism for all SCA exemptions foreseen by the law, subject to a positive risk analysis and without prejudice to the RTS on SCA[2].

The handling of SCA exemptions for transaction assets relies on several factors:

- the properties or context of the transaction whose initiation is being requested, especially as specified by the regulation (see below the list of exemptions as specified by the RTS on SCA).
- the need for an “as smooth as possible” customer journey.
- the need for a well-balanced risk-based analysis of this transaction.

In the context of PSD2, the Asset Holder, being liable and having to support the consequences of a dispute, is the actor who usually decides whether or not to apply an SCA exemption.

[1] https://www.europeanpaymentscouncil.eu/document-library/rulebooks/sepa-payment-account-access-spaa-scheme-rulebook

[2] Commission Delegated Regulation (EU) 2018/389 with regard to regulatory technical standards for Strong Customer Authentication and common and secure open standards of communication.

In the context of the Scheme, Asset Holders shall apply all SCA exemptions which they have implemented and a dialog between the Asset Broker and the Asset Holder will improve the handling of SCA exemptions by enabling the Asset Broker to play a more active role.

For the case of the non-risk-based exemptions of the RTS on SCA (Art. 10-17), this means that they must be applied to any given transaction, without any liability shift, unless

- it is not in scope of the RTS on SCA exemptions; or
- the Asset Holder's risk policy suggests otherwise; or
- the Asset Broker has requested to apply SCA.

For the case of the risk-based exemptions (RTS on SCA Art. 18), the following situations might arise:

- The Asset Broker might ask the Asset Holder to apply an SCA exemption, e.g. for the sake of a smooth customer journey.
- The Asset Broker might ask the Asset Holder not to apply an SCA exemption, e.g. when the risk-based analysis performed by the Asset Broker suggests a likelihood of fraud.
- The Asset Broker might provide a simple hint of whether or not to apply an SCA exemption.
- The Asset Broker might stay silent.

These different situations, combined with the context of the transaction, may induce several consequences, as described in the following table.

	The Asset Broker asks explicitly for an SCA exemption	**The Asset Broker asks explicitly for an SCA**	**The Asset Broker makes a recommendation or stays silent**
Non-risk-based exemptions of the RTS on SCA (Art. 11-17)	The Asset Broker has computed its own risk-based analysis. The Asset Holder applies a simple Authentication and leaves the risk to the Asset Broker. There is a liability shift since the Asset Holder's risk-based analysis may have raised a likelihood of fraud. In case of dispute the Asset Broker will have to reimburse the funds to the Asset Holder. Warning: the global amount cannot be computed by the sole Asset Broker , since the Payer may have initiated other low-value	The Asset Broker has computed its own risk-based analysis which raises a risk. The Asset Holder applies a Strong Authentication. There is NO liability shift.	The Asset Broker might provide the Asset Holder with its own assumption (e.g. risk score) about the need to process an SCA. The Asset Holder applies the exemption unless their risk-based analysis suggests otherwise. There is NO liability shift.

	payments through other channels		
Risk-based exemptions (RTS on SCA Art. 18)	The Asset Broker has computed its own risk-based analysis. The Asset Holder applies a simple Authentication. There is a liability shift. In case of dispute the Asset Broker will have to reimburse the funds to the Asset Holder. The statistics provided to the European Baking Authority (EBA) about risk should be taken by the Asset Broker and not by the Asset Holder.	The Asset Broker has computed its own risk-based policy which raises a risk. The Asset Holder applies a Strong Authentication. There is NO liability shift.	The Asset Holder processes a risk-based analysis and decides whether or not it will apply a Strong Authentication There is NO liability shift.

2.2.3.2 Directory Service

Within the PSD2 context, there are a number of situations where an SCA exemption can be granted by the ASPSP (Asset holder in SPAA context). The Directory Service would provide information on what SCA exemptions are implemented by the Asset Holder.

2.2.3.3 SCA and SCA exemption handling dataset

a. **API Request Dataset**

Identification:	**DS-36**
Name:	**Asset Broker request or suggestion about SCA handling**
Description:	This Dataset describes the minimum API attribute requirements related to the handling of SCA. It aims to communicate to the Asset Holder the Asset Broker's suggestion or request about SCA handling for a given payment initiation request as well as for providing consent for accessing data assets.
Attributes contained globally	• AT-A010 Reference of the payment initiation request (API resource ID) (O)
	• AT-A073 Asset Broker's consideration about SCA handling (O)
Technical characteristics	Since the SCA handling possibilities are exclusive one from the others, the relevant attribute is described here as an enumeration of those possibilities. However, this does not imply that the API Standardisation Initiatives will have to specify this as an API enumeration. Other technical choices could be applied.

Identification:	**DS-36**
Name:	**Asset Broker request or suggestion about SCA handling**
	The reference of the payment initiation request could be implicitly given.
Rules applied:	In case of SCA/SCA exemption requests, they have to be considered as prescriptive for the Asset Holder, subject to the business rules. In case of SCA/SCA exemption suggestions, they can be ignored by the Asset Holder.
Remarks	

b. **API Response Dataset**

Identification:	**DS-37**
Name:	**Asset Holder effective SCA handling**
Description:	This Dataset describes the minimum API attribute requirements related to the handling of SCA. It aims to communicate to the Asset Broker the Asset Holder's effective SCA handling for a given payment initiation request.
Attributes contained globally	• AT-A010 Reference of the payment initiation request (API resource ID) (M)
	• AT-A074 Asset Holder's effective SCA handling (M)
	• AT-A075 Liability shift indicator (O)
Technical characteristics	Since the SCA effective handling are exclusive one from the others, the relevant attribute is described here as an enumeration of those possibilities. However, this does not imply that the API Standardisation Initiatives will have to specify this as an API enumeration. Other technical choices could be applied.
Rules applied:	If the Asset Broker does not accept the liability shift indicator provided by the Asset Holder, the Asset Broker would have to ask to cancel the payment request.
Remarks	

2.2.3.4 Payer Identification and Authentication

Note: Further details about this topic can be found in the annex of document EPC164-22 API Security Framework[3].

2.2.3.4.1 Payer Identification

[3] The annex of document EPC164- 22 API Security Framework is currently being developed and expected to be available in Q2 2023.

A Payer identifier is required to uniquely identify the user that is entitled to access the Asset (data and transaction Asset). The Payer identifier has to be meaningful to both the Asset Holder and Asset Broker and is a prerequisite before applying Authentication (weak or strong).

2.2.3.4.2 Payer Authentication

The purpose of Payer Authentication (weak or strong through SCA) is for the authorisation of the performance of transaction and data Asset services. This Authentication is not related to Know Your Customer (KYC) processes, which are beyond the scope of the Rulebook.

The Authentication aims to prove the identification of the Payer and involves the use of one or more Authentication factors that are strictly specific to the Payer.

Authentication factors that can be used include:

- Knowledge (e.g., password).
- Possession (e.g., a device such as a smartphone).
- Inherence (e.g., a biometric challenge).

The Authentication process may be implemented:

- either as a weak Authentication wherein the Payer only needs to use just one Authentication factor, or
- as a strong Authentication wherein, the Payer will have to use at least two independent Authentication factors. At the time of writing the EBA interprets that the Authentication factors should be from a different category.

2.3 SCA approaches

At least one of the following SCA approaches should be implemented by the Asset Holder with the aim of coming up with a best practice for user experience.

The Authentication can be processed through different interaction scenarios called Authentication approaches. The eligible SCA approaches are listed in section 2.3.3 below[4].

An Authentication approach may involve different Authentication technologies or methods (e.g. biometrics, m-TAN,..) that are not described here due to fast evolving technology.

Moreover, these technologies or methods apply only between the Payer (being authenticated) and the Scheme Participant (performing the Authentication). For the embedded SCA, Authentication related information is only communicated by the Asset Broker. Thus further details are out of scope of the Scheme.

2.3.1 Need for a Two-Factor Authentication / Strong Customer Authentication

The RTS on SCA, with the aim to enforce the security, especially on the Payer's side, has stated that the default authentication procedure should be a "Two-Factor Authentication" or "Strong Authentication".

2.3.2 Business Rules

[4] This refers to section 2.3 SCA approaches of version 1.0 of the SPAA scheme rulebook (https://www.europeanpaymentscouncil.eu/document-library/rulebooks/sepa-payment-account-access-spaa-scheme-rulebook)

As mentioned in the Working Group on a SEPA Application Programming Interface (API) Access Scheme, to ensure high adoption and a good customer experience, any SCA-obliged party shall apply the best practice of the implemented SCA approaches, both from a usability and security perspective. Secure storage of the identity and the authorisation / Authentication credentials of the customer shall not be compromised.

Delegated SCA enables Asset Brokers to provide a 'lowest friction' mechanism for user Authentication processes. This mechanism is therefore strongly encouraged but it shall however not be mandated given the legal and contractual obligations (e.g., liability shift) related to the outsourcing of this functionality.

However, at least one of the eligible SCA approaches (see below section) should be implemented by the Asset Holder.

2.3.3 List of eligible SCA approaches

2.3.3.1 Delegated SCA with liability shift rules

Delegated SCA refers to an arrangement (e.g., a bilateral agreement) whereby the Asset Broker requests the Asset Holder to delegate its own SCA obligation. Upon Asset Holder's agreement, the SCA is then performed by the Asset Broker who takes the liability of fraudulently authorised transactions. The delegation arrangement could for example contain mechanisms for revocation of the delegation with limited or no notice to prevent detriment to Payers.

Sample SCA flow:

Step	Description
1	The Asset Broker performs itself the strong Authentication of the Payer.
2	The Asset Broker then sends to the Asset Holder the signed proof of this Authentication embedding: • The unambiguous identification of the Payer. • The timestamp of the Authentication. • The strength of the Authentication. • The category of each Authentication factor having been challenged. • The Asset Broker's relevant claims.
3	The Asset Holder checks the Authentication proof and performs the Asset Broker's claim.

2.3.3.2 Decoupled

The following three business scenarios can be distinguished after completing the check-out:

- App2app (m-commerce).
- Web2app (e-commerce).
- POS2app (in-store commerce).

The decoupled Authentication is done on a separate (decoupled) device or app, which is woken up by the Asset Holder based on the payment initiation or account information request of the Asset Broker only via the API.

Sample SCA flow:

Step	Description
1	The Asset Broker sends its request to the Asset Holder. The request embeds the unambiguous identification of the Payer.
2	Based on the identification, the Asset Holder alerts the relevant Payer on a registered device (e.g., smartphone) which will be considered as a possession factor.
3	The Payer opens the Asset Holder application and completes the Authentication through an eligible second factor.

2.3.3.3 Redirection

The following two scenarios can be distinguished:

- App2app: after completing the checkout in an m-commerce scenario, shoppers can perform SCA with one touch using their Authentication app triggered by the merchant / Asset Broker app.

Sample SCA flow:

Step	Description
1	On the Payer's smartphone, the Asset Broker's application will launch the Payer's Authentication application.
2	The Payer's Authentication application recognises the smartphone as a first authentication factor (possession). Then, this application requires the Payer to perform a second eligible Authentication factor challenge.
3	The Payer's Authentication application calls back the Asset Broker's application with the result of the Authentication.

- Web2web: after completing the checkout in an e-commerce scenario, shoppers can perform SCA with legacy web redirection triggered by the merchant / Asset Broker web page.

  Sample SCA flow:

Step	Description
1	The Payer, through the browser, is redirected by the Asset Broker to the Asset Holder's web domains.
2	There, the Payer usually enters a knowledge factor. Then, the Asset Holder will require the Payer to perform a second eligible Authentication factor challenge.
3	The Payer is afterwards redirected back to Asset Broker with the result of the Authentication.

2.3.3.4 Embedded SCA (with or without signed payment request)

The following two scenarios can be distinguished:

- Embedded without signed payment request: after completing the checkout in an e-&m- or in-store/POS-commerce scenario, shoppers can perform SCA depending on the use case

with or without (mobile) network coverage. Authentication factors are communicated via the API and details are left to API definitions.

Sample flow:

Step	Description
1	The Asset Broker sends its request to the Asset Holder. The request embeds the unambiguous identification of the Payer and usually a knowledge factor.
2	The Asset Holder can send challenge data via the Asset Broker to the Payer or send a One Time Password (OTP) related data directly to the Payer via a different channel.
3	The Payer types in the OTP as a possession factor within the Asset Broker's interface.
4	The Asset Broker sends the OTP back to the Asset Holder.
5	The Asset Holder returns the Authentication result to the Asset Broker.

- Embedded with signed payment request: after completing the checkout in an e-&m- or in-store/POS-commerce scenario, shoppers can perform SCA with one touch - depending on the use case with or without (mobile) network coverage - using their Authentication app triggered by the Asset Broker.

Sample flow:

Step	Description
1	The Asset Broker presents its claims to the Payer and asks for consent through an electronic signature process.
2	This electronic signature process embeds the use of a possession factor (the signing device or application) and an eligible second factor, e.g., fingerprint.
3	The signed consent, wrapping the claims, is then forwarded to the Asset Holder that will verify the signature(s) and apply the claims.
4	The Asset Holder returns the Authentication result to the Asset Broker

3 Request for feedback

All interested stakeholders are invited to participate in the public consultation by sending their comments on the extension of SCA sections in version 1.0 of the SPAA scheme rulebook via e-mail to spaa@epc-cep.eu by **15 March 2023 (midnight Brussels time)** at the latest. Kindly note that the EPC will not consider any feedback received after this deadline.

To submit your feedback on the draft rulebook, please use the response template (EPC285-22).