EBA-Op-2018-04

13 June 2018

Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC

Introduction and legal basis

1. The competence of the European Banking Authority (EBA) to deliver this opinion is based on Article 29(1)(a) of Regulation (EU) No 1093/2010[1] as part of the objective of the EBA to 'play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union'.

2. In order to support the objectives of Directive (EU) 2015/2366 (PSD2) of enhancing competition, facilitating innovation, protecting consumers, increasing security and contributing to a single EU market in retail payments, the Directive conferred on the EBA the development of 12 technical standards and guidelines, to specify detailed provisions in relation to payment security, authorisation, passporting, supervision and more.

3. The regulatory technical standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC) underpin the new security requirements under PSD2 and regulate the access by account information service providers (AISPs) and payment initiation service providers (PISPs) to customer payment account data held in account servicing payment service providers (ASPSPs). The RTS were published in the Official Journal on 13 March 2018[2] and will legally apply from 14 September 2019.

4. In order to fulfil its statutory objective of contributing to supervisory convergence in the EU/EEA, and to do so in the specific context of the RTS, the EBA has decided to issue an opinion in order to respond to a number of the numerous queries the EBA and competent authorities

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJEU L 331, 15.12.2010, p. 12).

[2] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (OJEU, L 69, 13.3.2018, p.23).

(CAs) have received from market participants and aims to provide clarity on the implementation of certain aspects of the RTS that were published. The opinion is addressed to CAs but, given the supervisory expectations it is conveying, should prove useful also for payment service providers (PSPs), payment schemes, technical service providers and industry initiatives, such as the application programming interface (API) initiatives that have recently been emerging across the EU to support the implementation of the RTS.

5. The opinion contains both general and specific comments to CAs in relation to the RTS on SCA and CSC. It focuses in particular on those queries for which clarity is required sooner, to enable industry players to continue in their preparations and to facilitate early readiness to comply with the RTS, which the EBA had already encouraged in its opinion on the transition from PSD1 to PSD2 in December 2017 (EBA/OP/2017/16).

6. Following the publication of this opinion, and of the separate Draft Guidelines on the criteria to assess exemptions from contingency measures under Article 33(6) of the RTS on SCA and CSC (EBA/CP/2018/09), the EBA will continue to provide clarifications, but aims to do so primarily through the use of the EBA's Single Rulebook question and answer (Q&A) tool, which will be extended to PSD2 by the end of June 2018, including the technical standards developed by the EBA[3].

7. In accordance with Article 14(5) of the Rules of Procedure of the Board of Supervisors[4], the Board of Supervisors has adopted this opinion, which is addressed to competent authorities.

General comments

8. In order for PSPs to be in a position to comply with the RTS on SCA and CSC by 14 September 2019, and to meet all preceding deadlines imposed by the RTS, industry participants will now need to develop or amend the necessary systems, hardware and software, including, in the case of ASPSPs, building interfaces and infrastructures. Clarity on the interpretation of the RTS requirements underpins building or adapting these infrastructures and systems in order to be compliant with the RTS, and facilitates consistent supervision of the RTS by CAs across the 28 EU Member States.

9. During their supervisory work, and given the content of some of the queries the EBA has received from market participants, CAs should remind the ASPSPs in their respective jurisdictions that ASPSPs are required to change and adapt their systems in response to the RTS, regardless of whether ASPSPs choose to modify the customer interface or to develop a dedicated interface. Where ASPSPs do not opt to implement the dedicated interface, their interface must still meet the various requirements under the RTS and PSD2, including the requirement for AISPs and PISPs to identify themselves.

[3] See https://www.eba.europa.eu/single-rule-book-qa

[4] Decision adopting the Rules of Procedure of the European Banking Authority Board of Supervisors of 27 November 2014 (EBA/DC/2011/01 Rev4).

10. Where ASPSPs choose to develop dedicated interfaces, this will require time, including the 6-month period laid down in the RTS[5] for other providers to be able to test the interface. In order to facilitate those developments, and to aim for consistency and a degree of standardisation in the industry, many initiatives have emerged across the EU to develop common functional and technical API specifications that provide assistance and some sort of toolbox for ASPSPs to use when developing their dedicated interfaces. This opinion may serve as a useful orientation for these initiatives when designing their standards in order to ensure that individual APIs created, based on these initiatives, are compliant with these requirements.

11. Chronologically, these toolboxes need to be available first for ASPSPs to be able to use them. ASPSPs will then need sufficient time for the testing and use of the individually implemented dedicated interface before the RTS apply, and for national CAs to review the interfaces and make a decision on whether or not the ASPSP should benefit from the exemption from the fallback under Article 33(6) of the RTS and the related EBA guidelines.

12. As part of its support for the development of such initiatives, and to facilitate convergence, consistency and standardisation across Europe, the EBA is of the view that, at a general level, the dedicated interface should ensure that the ASPSP developing the platform, as well as card-based payment instrument issuers (CBPIIs), AISPs and PISPs (which include credit institutions, PIs and EMIs that may wish to provide account information and/or payment initiation services) can comply with all their obligations under the RTS and PSD2. These obligations include, but are not limited to, the list contained in Table 1.

Table 1. Main requirements for dedicated interfaces and API initiatives

Requirement	**Article**
Enabling CBPIIs, AISPs and PISPs to access the necessary data from payment accounts accessible online	Articles 65, 66 and 67 PSD2 Article 30 RTS
Conforming to (widely used) standard(s) of communication issued by international or European standardisation organisations	Article 30(3) RTS
Allowing the payment service user (PSU) to authorise and consent to a payment transaction via a PISP	Article 64(2) PSD2 Article 30(1)(c) RTS
Enabling PISPs and AISPs to ensure that, when they transmit the personalised security credentials issued by the ASPSP, they do so through safe and efficient channels	Articles 66(3)(b) and 67(2)(b) PSD2
Enabling the identification of the AISP/PISP/CBPII and supporting eIDAS certificates	Articles 65(2)(c), 66(2)(d) and 67(2)(c) PSD2 Articles 30(1)(a) and 34 RTS
Allowing 90-day reauthentication for AISPs	Article 10(2)(b) RTS
Enabling the ASPSPs and AISPs to count the number of access requests during a given period	Article 36(5) RTS
Allowing a change control process	Article 30(4) RTS
Allowing the possibility of cancelling an initiated transaction in accordance with PSD2, including recurring transactions	Articles 64(2), 80(2) and 80(4) PSD2
Allowing error messages explaining the reason for the unexpected event or error	Article 36(2) RTS
Supporting access via technology service providers on behalf of authorised actors	Article 19(6) PSD2

[5] Note that the EBA is of the view that the 3-month 'widely used' period referred to in Article 33(6)(c) of the RTS on SCA and CSC may be included in this 6-month period.

Allowing AISPs and PISPs to rely on all authentication procedures issued by the ASPSP to its customers	Article 97(5) PSD2 Article 30(2) RTS
Enabling the AISP to access the same information as is accessible to the individual consumer and corporates in relation to their designated payment accounts and associated payment transactions	Article 67(2)(d) PSD2 Articles 30(1)(b) and 36(1)(a) RTS
Enabling the ASPSP to send, upon request, an immediate yes/no confirmation to the PSP (PISP and CBPII) on whether or not there are funds available	Article 36(1)(c) RTS
Enabling dynamic linking to a specific amount and payee, including batch payments	Article 97(2) PSD2 Article 5 RTS
Enabling the ASPSP to apply the same exemptions from SCA for transactions initiated by PISPs as when the PSU interacts directly with the ASPSP	Articles 18(2)(c)(v) and (vi), 18(3), 30(2) and 32(3) RTS
Enabling SCA composed of two different elements	Article 4 RTS
Enabling a secure data exchange between the ASPSP and the PISP, AISP and CBPII, mitigating the risk of any misdirection of communication to other parties	Articles 28 and 35 RTS
Ensuring security at transport and application levels	Article 97(3) PSD2 Articles 30(2)(c) and 35 RTS
Supporting the needs to mitigate the risk of fraud, have reliable and auditable exchanges and enable providers to monitor payment transactions	Article 97(3) PSD2 Articles 3, 22 and 35 RTS
Allowing traceability	Article 29 RTS
Allowing the ASPSP's dedicated interface to provide at least the same availability and performance as the user interface	Article 32 RTS

13. It is the EBA's view, after discussing it with the Commission, that, where AIS or PIS are provided to a payment service user (PSU) following a contract that has been signed by both parties, ASPSPs do not have to check consent. It suffices that AISPs and PISPs can rely on the authentication procedures provided by the ASPSPs to the PSU, when it comes to the expression of explicit consent.

14. The EBA also notes that regulated entities as well as other market participants that provide services to, or underpin the functioning of, payment services, such as payment schemes and technical service providers, are seeking clarification in a number of areas, and in particular with regard to SCA and the exemptions from SCA.

Specific comments

15. These specific comments refer to some of the requirements in the RTS, with the aim of providing clarity to CAs so that they can ensure that the PSPs they supervise implement the RTS in a way that is compliant with both the RTS and the underlying provisions in the Directive.

16. The EBA has identified the following specific areas as requiring clarity: the data that AISPs and PISPs can access, limitations to the frequency of access, methods of access, the application of SCA and the exemptions from it, and the method(s) of carrying out SCA.

The scope of data and four-times-daily limit

17. A number of existing AISPs, PISPs and ASPSPs (when providing AIS and/or PIS) are accustomed to accessing a large range of data through the use of what is commonly referred to as 'screen scraping'. For PISPs, this is particularly important if the ASPSP executing the payment does not

have any real-time booking system (i.e. a booking system immediately reflecting any movements on the account), as they seek confirmation from the ASPSP that the payment they are initiating will be executed.

18. With regard to AISPs, in practical terms, they tend to access different types of data including but not exclusively limited to data derived from payment accounts. Under Article 67(2)(d) PSD2, AISPs 'access only the information from designated payment accounts and associated payment transactions'. The RTS, in Article 36(1)(a), specify that AISPs have access to the same data as customers would be able to access in relation to their designated payment accounts and associated payment transactions using their web interface or mobile (or tablet) app, provided that this information does not include sensitive payment data. PSD2 is silent on access to other types of information than the information from payment accounts (and associated transactions).

19. The data that payment account holders themselves can see, at present and also once the RTS apply, are likely to comprise a core set of data that is common across most providers but there may be variation between them. This means that the data AISPs may access may vary depending on the ASPSP where the payment account is held.

20. The extent and scope of data may also vary depending on the channel used by the customer (and in particular between web interface and mobile (or tablet) app). The EBA clarifies that the AISPs can access the maximum amount of data available to PSUs with regard to their payment account(s) held with a specific ASPSP regardless of the electronic channel (e.g. mobile application or web) used to access it. In other words, if there are more data available through a computer connection online than through a mobile app, the AISP is able to access via the interface data available on the computer online regardless of the channel used by the PSU to access the AISP.

21. With regard to PISPs, Article 66(3)(f) and (g) of PSD2 state that the PISP shall 'not request from the payment service user any data other than those necessary to provide the payment initiation service' and shall 'not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer', while Article 66(4)(b) states that the ASPSP shall 'provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider'.

22. Furthermore, Article 36(1)(b) of the RTS states that ASPSPs shall provide PISPs 'with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user'. In addition, Article 36(1)(c) of the RTS requires ASPSPs to provide immediate confirmation of whether or not there are funds available at the provider's request, in a 'yes or no' format. The EBA wishes to clarify that Article 36(1)(c) applies to PSPs including CBPIIs and PISPs, rather than solely CBPIIs.

23. The EBA would also like to clarify that the combination of Article 36(1)(b) and (c) establishes legally binding requirements that are aimed at ensuring that the provider initiating a payment has the information it needs to initiate a payment as requested by the PSU. The yes/no answer will help the PISP to manage the risk it may face if, following the initiation of the payment, it transpires that the payment cannot be executed. It may not be possible to assess this risk with only the information received under Article 36(1)(b) of the RTS.

24. Neither PSD2 nor the RTS make any distinction between payments processed through real-time booking or through delayed (or batch) booking. However, in practical terms, PISPs may have a particular interest in seeking reassurance as to the likelihood that the payment will be executed in the latter case, given that in the absence of a real-time booking system there might be more uncertainty on the status of the initiated transaction.

25. In this context, the EBA considers that the ASPSP, in determining whether to give a yes or no response to the request for confirmation required under Article 36(1)(c), needs to determine whether or not there are funds available taking into account not only the balance available but also any overdraft and also any other data that the ASPSP uses to determine whether or not to execute a payment of one of its own customers, for instance any incoming/outgoing payments that will affect the balance or overdraft.

26. In the event that the ASPSP does not have a system that enables it to adequately respond to the confirmation request sent by the provider initiating the payment, then the ASPSP should give PISPs the possibility of accessing the necessary data themselves, so as to allow them to make their own judgements on the sufficient availability of funds.

27. Additionally, the EBA clarifies that the scope of data to be shared with AISPs and PISPs by the ASPSP under PSD2 and the RTS on SCA and CSC does not include the PSU's identity (e.g. address, date of birth, social security number) given that those are not data that are necessary or requested to initiate a payment or access account information under PSD2.

28. The EBA also notes that Article 36(5)(b) RTS limits the AISP's access to payment account data without the customer being directly involved to four times a day. A PSU will not be directly involved if it is not in a session at the time of the request, i.e. not actively viewing the data or executing an action to refresh the data to be displayed. An ASPSP may contractually agree with the AISP that the AISP can access the account without the customer's involvement at 'a higher frequency', or for the ASPSP to push information to the AISP, 'with the payment service user's consent'.

29. Given that PSD2 does not limit the types of payment transactions a PISP is allowed to offer, and given the provisions in Articles 4(15) and 66(1) of PSD2 in particular, the EBA would like to clarify that a PISP has the right to initiate the same transactions that the ASPSP offers to its own PSUs, such as instant payments, batch payments, international payments, recurring transactions, payments set by national schemes and future-dated payments.

The application of SCA

30. One of the fundamental changes introduced by PSD2 is to formalise payment security requirements in national law.

31. While SCA has in practice been applied in a number of EU Member States, including through the EBA guidelines on the security of internet payments under PSD1 (EBA/GL/2014/12_Rev1)[6], which continue to apply until the RTS on SCA and CSC under PSD2 apply from 14 September 2019 onwards, a number of Member States have not yet applied those requirements and, in those that have, the scope has often been more limited, given that the EBA guidelines applied only to online payments. This means that the requirement under PSD2 for all payment service providers to apply SCA when initiating or executing (acquiring in the context of card payments) electronic payment transactions will require changes, especially when taking the evolution of technology into account.

SCA and two-factor authentication

32. As explained in the final report on the draft RTS published in February 2017, the EBA's view, after discussing it with the European Commission, is that SCA applies to all payment transactions initiated by a payer, including to card payment transactions that are initiated through the payee within the EEA and apply only on a best-effort basis for cross-border transactions with one leg out of the EEA. In such a case, the liability regime stated by Article 74(2) PSD2 applies.

33. SCA is defined in PSD2 as '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' and that 'protect[s] the confidentiality of the authentication data'. Articles 6 to 9 of the RTS provide further detail and requirements. The EBA considers that the two factors need to belong to two different categories.

34. Payment service providers therefore need to devise an authentication method that uses two elements from two different categories, for instance one element categorised as knowledge (such as a password) and one as inherence (such as fingerprints). An element based on inherence is typically based on biometrics (including behavioural biometrics), provided they comply with the requirements under Article 8 of the RTS.

35. Given that knowledge is defined as 'something only the user knows', the card number with CVV and expiry date printed on the card cannot be considered a knowledge element. This is also the case for a user ID. For a device to be considered possession, there needs to be a reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device.

[6] https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29.pdf/f27bf266-580a-4ad0-aaec-59ce52286af0

36. SCA has to be applied to access to payment account information and to every payment initiation, including within a session in which SCA was performed to access the account data, unless an exemption under the RTS applies.

Who can apply SCA and who can decide?

37. Article 97(5) of PSD2 states that the ASPSP shall allow PISPs and AISPs to rely on the authentication procedures provided to its PSUs and Article 67(2)(b) states that the security credentials are accessible to the AISPs and PISPs. Recital 30 of PSD2 also states that 'The personalised security credentials used for secure customer authentication by the payment service user or by the payment initiation service provider are usually those issued by the account servicing payment service providers'.

38. The articles mentioned above are to be read in conjunction with one another, which means that the PSP applying SCA is the PSP that issues the personalised security credentials. It is consequently also the same provider that decides whether or not to apply an exemption in the context of AIS and PIS. The ASPSP may, however, choose to contract with other providers such as wallet providers or PISPs and AISPs for them to conduct SCA on the ASPSP's behalf and determine the liability between them. The EBA also notes that a number of governmental (national) agreements on universal sets of personalised security credentials that can be used by PSUs with multiple PSPs already exist in some Member States.

39. The EBA notes that PISPs and AISPs sometimes wish to issue their own credentials for accessing their own platform (e.g. app or online website) and may therefore also wish to decide whether or not to perform authentication procedures for accessing this platform. However, only the ASPSP can apply SCA or decide whether or not an exemption applies to a PSU's payment account in the context of AIS and PIS. For instance, only the ASPSP can decide whether or not to apply the transaction risk analysis exemption under Article 18 of the RTS. The PISP may have access to the list created and/or amended by the PSU in the ASPSP's domain but the decision whether or not to apply the exemption remains with the ASPSP.

Exemptions from the SCA requirement

40. With regard to the use of the exemptions under Articles 10 to 18 of the RTS on SCA and CSC, the EBA hereby clarifies that payees can never decide whether or not to use an exemption. Table 2 provides an overview of whether or the payer's PSP (issuer) and the payee's PSP (acquirer) can decide on each of the exemptions set out under Articles 10 to 18.

Table 2. Summary table on who may apply an exemption

RTS article	Exemption	Payer's PSP	Payee's PSP	
			Credit transfers	Cards
Access to information	Access to payment account information	Yes	N/A	N/A
Article 11	Contactless payments at POS	Yes	No	Yes*
Article 12	Unattended terminal for transport and parking	Yes	No	Yes*
Article 13	Trusted beneficiaries	Yes	No	No
Article 14	Recurring transactions	Yes	No	Yes*
Article 15	Credit transfers to self	Yes	No	N/A
Article 16	Low-value transactions	Yes	No	Yes*
Article 17	Secure corporate payment processes and protocols	Yes	No	N/A
Article 18	Transaction risk analysis	Yes	No	Yes*

*The payer's PSP always makes the ultimate decision on whether or not to accept or apply an exemption; the payer's PSP may wish to revert to applying SCA to execute the transaction if technically feasible or decline the initiation of the transaction.

41. The exemption in Article 10 relates to access to data in general. The other provisions relate to exemptions from SCA in relation to payment transactions. The exemptions in relation to payment transactions are separate and independent from one another, and only one exemption needs to be applied for any given transaction, even if the given transaction could qualify for more than one exemption.

42. This means that for the purpose of Article 11 or 16, for example, the limit of five transactions needs to be calculated not on the basis of all transactions where the exemption could have been applied but on the basis of transactions where the particular exemption was applied.

43. On a separate note, a number of market participants have expressed confusion with regard to the two cumulative limits set in Articles 11 and 16 of the RTS and in particular whether or not both the limit based on the number of transactions (five) and the limit based on the monetary amount (EUR 150 and EUR 100 respectively) shall be met, following a number of drafting iterations of the RTS. The EBA hereby clarifies that the cumulative limit is either the limit based on the number of transactions or the monetary amount (but not both). This means that it may be preferable for PSPs to decide at the outset which cumulative limit they use (rather than on a transaction-by-transaction basis), as it may otherwise be confusing for consumers. They should also ensure that their systems and other technical solutions used to provide a particular service cater for this possibility.

44. Article 10 of the RTS on SCA and CSC provides an exemption from SCA when a PSU or AISP accesses limited payment account information (namely the balance or data on the last 90 days of payment transactions) for a period of 90 days after the first initial access using SCA. The 90-day period is specific to each AISP and is also separate from the 90-day period for the PSU directly accessing its account information. When the period of 90 days has lapsed, the exemption no longer applies and SCA needs to be performed again for the new 90-day period to start. The ASPSP can reset the 90-day counter whenever SCA is applied, regardless of the channel (e.g. web browser or app) the PSU uses to access its account. Making a payment

directly or via payment initiation and performing SCA will not restart the 90-day counter for the purpose of Article 10. Providers, as well as API initiatives where applicable, need to accommodate a counter for these 90 days; alternatively a response code indicating that the 90-day limit has been exceeded could be put in place.

45. With regard to the exemption on trusted beneficiaries (Article 13), the EBA clarifies that the exemption is not limited to credit transfers and may apply to cards through the payer's PSP, upon the payer's confirmation. The EBA also clarifies that the payee's PSP cannot apply this exemption and that a payee could not have such a list for the purpose of the exemption (e.g. cards on file), as illustrated in Table 2 above.

46. Article 18 allows a PSP not to use SCA in the case of low-risk transactions where transaction risk analysis has been used, provided that the fraud rate is below a given threshold defined in Article 19(1)(2) of the RTS and Annex A of the RTS. Article 19(1), second paragraph, of the RTS states that the fraud rate 'shall be calculated as the total value of unauthorised or fraudulent remote transactions'. The EBA clarifies that the fraud rate includes not only unauthorised transactions but also fraudulent transactions resulting from the manipulation of the payer as proposed to be defined in the Consultation Paper on the EBA Guidelines on fraud reporting (EBA-CP-2017-13), which the EBA will be finalising in summer 2018[7]. In the case of transactions processed by more than one PSP (e.g. card transactions), the EBA would also like to clarify that the fraudulent transactions included in the calculation for a given PSP's fraud rate should be based on (i) the unauthorised transactions for which the given PSP has borne liability, as determined in accordance with Article 74 of PSD2, and (ii) other fraudulent transactions which have not been prevented by that PSP.

47. The fraud rate as defined in Annex A of the RTS is calculated for all credit transfer transactions and all card payment transactions and cannot be defined per individual payee (e.g. merchant) or per channel (whether app or web interface). The fraud rate that determines whether or not a PSP qualifies for the SCA exemption cannot be calculated for specific merchants only, i.e. where the payer wants to make a payment to a specific merchant and this specific merchant has a fraud risk that is below the threshold. While the payee's PSP (acquirer) may contractually agree to 'outsource' its transaction risk analysis monitoring to a given merchant, or allow only certain predefined merchants to benefit from that PSP's exemption (based on a contractually agreed low fraud rate), the fraud rate making a given PSP eligible for an exemption under Article 18 would still need to be calculated on the basis of the payee PSP's executed or acquired transactions, rather than on the merchant's transactions.

Method(s) of carrying out SCA

48. There would appear to currently be three main ways or methods of carrying out the authentication procedure of the PSU through a dedicated interface, and APIs in particular, namely redirection, embedded approaches and decoupled approaches (or a combination

[7] http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

thereof). In the cases of redirection and decoupled approaches, PSU's authentication data are exchanged directly between PSUs and ASPSPs, as opposed to embedded approaches, in which PSU's authentication data are exchanged between TPPs and ASPSPs through the interface. In a number of national markets, many ASPSPs have traditionally used redirection, while other markets have used a more embedded approach.

49. Redirection is mentioned in the RTS under Article 32(3), and its featuring in the RTS has generated some debate in the industry, with some market participants expressing the view that the reference suggested that redirection would be an obstacle to the provision of AIS and PIS. The EBA hereby clarifies that the RTS do not state that redirection per se is an obstacle to AISPs and PISPs providing services to their PSUs. Instead, the RTS state that it 'may' be so, if the ASPSP implements it in a manner which is restrictive or obstructive for AISPs or PISPs.

50. When determining which method(s) to use for the purpose of carrying out the authentication procedure, in line with Article 97(5) PSD2 and Article 30(2) of the RTS, all methods of SCA provided to the PSU need to be supported when an AISP or PISP is used. If they were not, this would constitute an obstacle. Therefore, which method, or combination of methods, any particular ASPSP needs to use will depend on the authentication procedures it offers to its own PSUs.

51. Finally, the EBA advises the CAs to encourage their market participants to use the EBA Q&A tool as soon as it becomes available to submit any query they may have in relation to the RTS on SCA and CSC.

This opinion will be published on the EBA's website.

Done at London, 13 June 2018

[signed]

Andrea Enria

Chairperson
For the Board of Supervisors