EBA/OP/2020/10

4 June 2020

Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC

Introduction and legal basis

1. Directive (EU) 2015/2366 on payment services in the internal market (PSD2) requires Member States to ensure that customers have the right to use the services of regulated third party providers (TPPs) offering account information services (AIS) and payment initiation services (PIS). To this end, the PSD2 and the regulatory technical standards on strong customer authentication (SCA) and common and secure communication (the RTS) require account servicing payment service providers (ASPSPs) to establish the access interfaces through which TPPs can access the customers' payment accounts in a secure manner, and to ensure that these comply with the applicable requirements in the PSD2 and the RTS. In accordance with Article 31 RTS, these access interfaces can be either a dedicated interface (in general an application programming interface or API) or the modified customer interface.

2. Article 32(3) of the RTS requires ASPSPs that have implemented a dedicated interface to ensure that the interface does not create obstacles to the provision of payment initiation and account information services. Article 32(3) provides a number of examples of what "may" constitute an obstacle, without being exhaustive.

3. 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 is issuing this opinion with a view of responding to a number of queries and issues that had been raised by market participants with the EBA and national competent authorities (NCAs) regarding the dedicated interfaces provided by ASPSPs and, in particular, regarding potential obstacles to the provision of TPPs' services. The EBA competence to deliver this opinion is based on Article 29(1)(a) of Regulation (EU) No 1093/2010[1], as part of the EBA's objective to "play an active role in building a

[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 (OJ L 331, 15.12.2010, p. 12).

common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union".

4. In accordance with Article 14(7) of the Rules of Procedure of the Board of Supervisors[2], the Board of Supervisors has adopted this opinion which is addressed to NCAs under the PSD2.

General comments

5. Since the application date of the RTS on 14 September 2019, a number of TPPs have reported issues regarding redirection approaches offered by ASPSPs, where the customer is redirected to the ASPSP in order to authenticate when using AISPs/PISPs services. The issues that have been raised in this context refer in particular to the scenario where redirection is the sole method of carrying out the authentication of the PSU supported by ASPSPs. A number of TPPs have argued that redirection is an obstacle for TPPs that want to offer their own user experience, if redirection is the only method of carrying out the authentication of the PSU that is supported by the ASPSP.

6. As clarified in the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04)[3] and the EBA Guidelines on the exemption from the contingency mechanism under Article 33(6) RTS (EBA/GL/2018/07)[4], the EBA is of the view that redirection is not, in itself, an obstacle, but that it may be an obstacle depending on the way it is implemented. The EBA clarifies that redirection can be an obstacle if implemented in a manner that creates unnecessary friction in the customer experience when using TPPs' services, or if the authentication procedure with the ASPSP is more cumbersome compared to the equivalent experience PSUs have when directly accessing their payment accounts or initiating a payment with the ASPSP.

7. The EBA also clarified in the final report on the above-mentioned Guidelines that, in a redirection or decoupled approach, where the PSU is redirected to the ASPSP to authenticate, the interaction between the PSU and the ASPSP should be minimised to what is necessary in order for the PSU to authenticate. The authentication procedure with the ASPSP as part of an AIS/PIS journey should not include unnecessary steps or require the PSU to provide unnecessary or superfluous information compared to the way in which the PSU can authenticate when directly accessing their payment accounts or initiating a payment with the ASPSP. The EBA deems such unnecessary steps or information required as obstacles.

Specific comments

8. Having assessed the requests it has received, the EBA has identified the following specific areas as requiring clarity:

[2] Decision adopting the Rules of Procedure of the European Banking Authority Board of Supervisors of 22 January 2020 (EBA/DC/2020/307).

[3] See: https://eba.europa.eu/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer-authentication-and-common-and-secure-communication

[4] See: https://eba.europa.eu/eba-publishes-final-guidelines-on-the-exemption-from-the-fall-back-mechanism-under-the-rts-on-sca-and-csc

- authentication procedures that ASPSPs' interfaces are required to support;
- mandatory redirection at the point-of-sale;
- multiple SCAs;
- 90-days re-authentication;
- account selection;
- additional checks on consent; and
- additional registrations.

Each issue will be addressed in turn below and clarifications provided accordingly.

9. The EBA expects NCAs to take into account the clarifications provided in this opinion in monitoring compliance of the interfaces provided by ASPSPs with the requirements in PSD2 and the RTS, as part of their supervisory work and ongoing monitoring under Articles 30(6) and 33(7) of the RTS. The EBA advises NCAs to pay particular attention in their assessment to the customer journey in redirection-based approaches, especially where redirection is the sole method of carrying out the authentication of the PSU that is supported by the ASPSP's interface. Where obstacles are identified, the EBA expects NCAs to take the necessary actions to ensure compliance with the PSD2 and the RTS, and ensure that ASPSPs remove any obstacles identified within the shortest possible time and without undue delay.

10. The EBA will monitor the way in which the clarifications provided in this opinion are taken into account, so as to contribute to a level playing field across the EU and to a consistent application of relevant requirements. Where the EBA identifies inconsistencies, despite the clarifications provided in this opinion (and the previous clarifications provided in the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04)[5], the EBA Guidelines on the exemption from the contingency mechanism under Article 33(6) RTS (EBA/GL/2018/07)[6] and Q&As), it will take the actions needed to remedy those inconsistencies, by making use of the powers conferred on the EBA in its founding regulation.

Authentication procedures that ASPSPs' interfaces are required to support

11. Article 30(2) RTS require ASPSPs to ensure that the access interfaces provided to TPPs in accordance with Article 30(1) RTS do not prevent account information service providers (AISPs) and payment initiation service providers (PISPs) from relying upon the authentication procedure(s) provided by the ASPSP to its PSUs. As clarified in EBA Opinion on the implementation of the RTS (EBA-Op-2018-04)[7] and the EBA Guidelines on the exemption from the contingency mechanism under Article 33(6) RTS (EBA/GL/2018/07)[8], this means that the method(s) of carrying out the authentication of the PSU (i.e. redirection, decoupled,

[5] See footnote 3.

[6] See footnote 4.

[7] See footnote 3.

[8] See footnote 4.

embedded or a combination thereof) that ASPSPs should support will depend on the authentication procedures made available by the ASPSP to its PSUs and should support all these authentication procedures.

12. As clarified in the fourth set of clarifications to the EBA working group on APIs under PSD2 published in July 2019[9], one of the consequences of the above is that ASPSPs that enable their PSUs to authenticate using biometrics when directly accessing their payment accounts or initiating a payment, and that require the PSU to authenticate with the ASPSP to use AISPs/PISPs' services, should also enable their PSUs to use biometrics to authenticate with the ASPSP in a PIS or AIS journey. Given that biometrics are not transmittable credentials, this means that these ASPSPs should enable their PSUs to authenticate with the ASPSP in an AISP or PISP journey using biometrics, by supporting decoupled authentication or app-to-app redirection to the ASPSP's authentication app, and secure transmission of the ASPSP's app authentication status to the ASPSP (e.g. using a signed proof that the biometric validation has been performed successfully).

13. Furthermore, in the EBA's view, it follows from Article 30(2) RTS that ASPSPs that enable their PSUs to authenticate using the ASPSP's mobile banking app or a dedicated/decoupled app, as one of the two-SCA factors categorised as possession, in line with paragraph 26 of the EBA Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06)[10], when directly accessing their payment accounts or initiating a payment with the ASPSP, and that require PSUs to authenticate with the ASPSP to use the AISPs/PISPs' services, should also enable their PSUs to use the ASPSP's authentication app as one of the two-factor SCA elements in an AIS or PIS journey.

14. If the interfaces provided by ASPSPs do not support all the authentication procedures made available by the ASPSP to its PSUs, this would be a breach of Article 30(2) RTS and an obstacle under Article 32(3) RTS.

15. Moreover, the authentication of the PSU with the ASPSP in an AISP/PISP journey, in a redirection or decoupled approach, should not create unnecessary friction or add unnecessary steps in the customer journey compared to the equivalent authentication procedure offered to PSUs when directly accessing their payment accounts or initiating a payment with the ASPSP.

16. It follows from the above that, if an ASPSP has implemented a redirection or decoupled approach and enables its PSUs to authenticate using the ASPSP's mobile banking app or a dedicated/decoupled app to directly access their payment accounts or initiate a payment, the ASPSP should enable that, when the PSU is using the services of an AISP/PISP via an app provided by the AISP/PISP,

[9] See: https://eba.europa.eu/eba-publishes-clarifications-to-the-fourth-set-of-issues-raised-by-its-working-group-on-apis-under-psd2

[10] See: https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2

(i) the PSU is redirected from the AISP/PISP’s app to the ASPSP’s authentication app, assuming the latter is installed on the PSU's device, without any additional and unnecessary steps in-between (such as the PSU being redirected first to the ASPSP’s mobile browser environment); and that

(ii) after authentication with the ASPSP, the PSU is automatically redirected back to the AISP/PISP’s app, without for example the PSU having to manually reopen the TPP’s app, which would be an obstacle.

17. If, however, in the scenario described in paragraph 16 above, the PSU is using the AISP/PISP’s services in a mobile browser environment, and not via the AISP/PISP’s app, the EBA does not consider it an obstacle if the PSU is redirected to the ASPSP’s mobile browser authentication page to enter their credentials, provided that this is the only way in which PSUs authenticate when directly accessing their payment accounts via the ASPSP’s mobile web browser environment.

Mandatory redirection at the point-of-sale

18. A number of market participants expressed the view that mandatory redirection is an obstacle for TPPs, particularly at the point-of-sale, because redirection only works in a web-browser or mobile apps-based environment and therefore limits the TPPs’ ability to design new ways in which customers can initiate payments. In the view of these market participants, in order for PIS to work at the point-of-sale, and to enable PISPs to compete with card payments at the point-of-sale, ASPSPs should be required to enable decoupled or embedded SCA flows.

19. The EBA would like to clarify that, as detailed in paragraph 15 above, mandatory redirection in an AIS/PIS journey is an obstacle if redirection is the sole method of carrying out the authentication of the PSU that is supported by an ASPSP and does not support all the authentication procedures made available by the ASPSP to its PSUs. Paragraphs 16 and 17 above provide some examples of cases where ASPSPs would need to implement a decoupled authentication or app-to-app redirection to support all authentication procedures offered by the ASPSP to its PSUs in accordance with Article 30(2) RTS.

20. However, the PSD2 does not oblige ASPSPs to implement an embedded approach, or to enable PIS-initiated payments using authentication procedures that the ASPSP does not yet offer to its PSUs.

21. This being said, the EBA would like to recall that, as clarified in paragraph 29 of the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04)[11], a PISP has the right to initiate the same transactions that the ASPSP offers to its own PSUs. This means that, if an ASPSP were to offer to its customers the possibility to perform instant payments at the point of sale

[11] See footnote 3.

directly, the ASPSP should also allow its customers to initiate instant payments, within the same amount limits, at the point of sale using PISPs' services.

Multiple SCAs

22. As mentioned in paragraph 15 above, the authentication of the PSU with the ASPSP as part of an AISP/PISP journey in a redirection or decoupled approach should not create unnecessary friction or add unnecessary steps in the customer journey, compared to the equivalent authentication procedure offered to PSUs when directly accessing their payment accounts or initiating a payment with the ASPSP. In the EBA's view, such unnecessary friction or steps are obstacles to the provision of TPPs' services.

23. In this context, requesting multiple SCAs can be an obstacle to the provision of TPPs' services, as further explained below. In an AIS-only journey, the authentication procedure with the ASPSP for PSUs to access their payment accounts through an AISP should not require more SCAs, or add unnecessary friction in the customer journey, compared to the authentication procedure offered to PSUs when directly accessing their payment accounts with the ASPSP.

24. In a PIS-only journey, the EBA arrived at the conclusion that ASPSPs should support a single SCA for a single payment initiation via a PISP, if the PISP transmits to the ASPSP all the information necessary to initiate the payment, including the account number/IBAN of the account to be debited. Requiring two SCAs in such a case, namely one SCA for accessing the account data, and a separate SCA for initiating the payment, is not necessary and is, therefore, an obstacle, unless the ASPSP has duly justified security arguments why two SCAs would be needed in such case, as further detailed in paragraph 26 below.

25. This follows because, in the given scenario, the account data accessed is limited to the data related to the specific payment initiated via the PISP. This is different from the scenario where the PSU directly initiates a payment with the ASPSP, where the PSU may access, upon logging in the ASPSP's online banking, other payment accounts data, and where a separate SCA may be necessary under Article 97(1)(a) PSD2 to access such data.

26. Requiring two SCAs in the PIS scenario described above is therefore an obstacle, unless the ASPSP has security arguments that are duly justified, such as suspicion of fraud for a particular transaction, and can substantiate, upon request, to its NCA why two SCAs would be needed in such a case. The fact that the ASPSP may require a separate SCA for 'log-in' when the customer directly initiates a payment with the ASPSP, is not a sufficient ground to justify applying two SCAs in the PIS scenario described, for the reasons explained above.

27. This being said, where the payment account to be debited is not transmitted by the PISP to the ASPSP in the payment initiation request, and is selected by the PSU on the ASPSP's domain, requiring two SCAs, namely one SCA to access the list of payment accounts, and a second SCA to authenticate the payment, is not an obstacle.

28. Two SCAs may also be required, without being an obstacle, in the case of a combined AIS and PIS journey. In such case, the EBA considers that two SCAs would be necessary, unless an exemption applies, namely one SCA in order to access the payment account data in accordance with Article 97(1)(a) PSD2, and a separate SCA in accordance with Article 97(1)(b) PSD2 in order to initiate the payment.

90 days re-authentication

29. A number of market participants have expressed concerns that the requirement for PSUs to carry out SCA with the ASPSP every 90-days, or more frequently, in order to use AISP's services can have a negative impact on AISPs' business, particularly where an AISP aggregates data from several payment accounts of the same PSU held with multiple ASPSPs, as the PSU would need to undertake SCA with each ASPSP in order for the AISP to continue having access to the account data. Some of these market participants have argued that, in order to mitigate the impact on AISPs' business, AISPs should be allowed to perform the subsequent SCA renewals, after the initial SCA with the ASPSP, either on the ASPSP's behalf or using AISP-issued credentials.

30. The EBA would like to recall that Article 97(1)(a) and 97(4) of PSD2 require SCA to be applied each time the PSU accesses their online payment account(s), either directly or through an AISP. Article 10 RTS provides an exemption from the requirement to apply SCA for each access, where the PSU or AISP accesses only limited set of data (namely only the balance and/or the payment transactions executed in the last 90 days). However, even under this exemption, PSUs are still required to re-authenticate at least every 90 days in order to confirm that the AISP can continue accessing their payment accounts data without SCA. The EBA set the 90 days re-authentication requirement to reach an appropriate balance between the competing objectives of PSD2 of ensuring consumer-friendliness and ease of use, on the one hand, and increasing security, on the other hand. The 90-days requirement itself is therefore not an obstacle.

31. In order to minimise friction in the customer journey, to mitigate the impact that a authentication with the ASPSP more frequently than 90 days may have on AISPs' services and to avoid potential obstacles, the EBA advises NCAs to encourage all their ASPSPs to make use of the Article 10 exemption, by supporting ongoing 90-day access by AISPs without SCA.

32. As regards the question of who can perform the renewal of SCA, as clarified in paragraphs 37 to 39 of the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04)[12], the EBA is of the view that the obligation and responsibility under PSD2 to perform SCA lies with the ASPSP. While ASPSPs may choose to delegate/outsource SCA to TPPs in order for them to conduct SCA on the ASPSP's behalf, ASPSPs are not obliged under PSD2 to do so. The EBA also recalls NCAs that, where the delegation of SCA to a third party constitutes an outsourcing of

[12] See footnote 3.

SCA, the requirements set out in the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)[13] apply.

Account selection

33. Some market participants raised queries about how the account selection should be handled in a redirection approach and reported instances where PSUs are required to manually input their IBAN in an AIS or PIS journey into the ASPSP's domain, a practice that these market participants consider as an obstacle.

34. The EBA clarifies that interface implementations that require PSUs to manually input their IBAN into the ASPSP's domain in order to be able to use AISPs/PISP's services are an obstacle.

35. There are different ways to avoid PSUs having to manually input their account details in a PIS or AIS journey. One option is for the ASPSP to enable TPPs that have an AIS license and that have obtained the PSU's consent as required under Article 67(2)(a) of PSD2 to retrieve the list of all the PSU's payment accounts via the interface, thus enabling the PSU to select the account on the TPP's domain. The TPP could then send a separate request to the ASPSP for account access or, as may be the case, payment initiation, with the relevant account details.

36. Alternatively, if the ASPSP has implemented a redirection or decoupled approach, and the TPP does not transmit to the ASPSP the relevant account details, the ASPSP could enable the PSU to select the account(s) on the ASPSPs' domain during the authentication procedure with the ASPSP, in a way that is no more complicated than the way in which the PSU can select the account(s) for directly accessing their payment accounts or initiating a payment with the ASPSP. For example, ASPSPs may consider offering a drop-down list for the PSU to select the account(s), or prepopulate the account details if the PSU has only one account with the ASPSP.

37. However, the latter of these two options is currently not supported in an embedded approach, i.e. where the PSU's authentication credentials are exchanged between the TPP and the ASPSP, and where the PSU does not interact with the ASPSP to authenticate. This means that, in the case of an embedded-only approach, a PISP that does not also have an AIS license and/or the necessary consent from the PSU to access the list of all the PSU's payment accounts, may need to obtain in advance from the PSU the details of the account from which the PSU wants to initiate the payment.

38. The EBA also clarifies that the ASPSP is not required to share with PISPs the list of all the PSU's payment accounts. In fact, a PISP is not entitled under PSD2 to access the list of all the PSU's payment accounts, as this information goes beyond the scope of data that PISPs have the right to access under Article 66(4)(b) PSD2 and Article 36(1)(b) RTS.

39. For these reasons, not providing the list of all payment accounts to a PISP is not an obstacle.

[13] See: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

40. However, where the PISP does not communicate to the ASPSP the IBAN of the PSU account to be debited, and the PSU selects the account on the ASPSP's domain, the ASPSP should provide to the PISP the number of the account that was selected by the PSU and from which the payment was initiated, in accordance with Article 66(4)(b) of PSD2 and Article 36(1)(b) RTS, if this information is also provided or made available to the PSU when the payment is initiated directly by the PSU.

41. If the IBAN of the payment account to be debited, or, respectively, of the payment account(s) to which the AISP requests access is transmitted by the PISP/AISP to the ASPSP, the ASPSP should not request the PSU to re-select the account on the ASPSP's domain. Requiring the PSU to reselect the account if such information was already transmitted by the PISP/AISP to the ASPSP is an obstacle. However, the simple display by the ASPSP of the account selected as part of the authentication procedure is not in itself an obstacle.

Additional checks on consent

42. A number of market participants raised queries on what constitutes an "additional check on consent" under Article 32(3) RTS, and reported cases where ASPSPs offer so-called "opt-in" features, requiring their PSUs to provide an upfront consent to the ASPSP to be able to use the TPPs' services, a practice that these market participants consider as an obstacle.

43. Article 32(3) RTS explicitly mentions additional checks of the consent given by PSUs to AISPs/PISPs as a potential obstacle. The EBA clarified in paragraph 13 of the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04)[14] and the final report on the EBA Guidelines on the exemption from the contingency mechanism under Article 33(6) RTS (EBA/GL/2018/07)[15] that it is the obligation of the PISP/AISP to ensure that it has obtained the PSU's explicit consent in accordance with Article 66(2) of PSD2 and, respectively, Article 67(2)(a) of PSD2, and that the ASPSP should not check the consent given by the PSU to the PISP/AISP. This was also confirmed by the European Commission in its response to Q&A 4309[16].

44. Therefore, a general, ex-ante consent required by the ASPSP in order for PSUs to be able to use the AISPs/PISPs' services is an obstacle under Article 32(3) RTS. The EBA would also like to recall that, as stated in recital 69 of PSD2, terms and conditions concluded by ASPSPs with their PSU "should not contain any provisions that would make it more difficult, in any way, to use the payment services of other payment service providers authorised or registered pursuant to [PSD2]".

45. This does not preclude the possibility for the PSU to request to the ASPSP to deny access to their payment account(s) to one or more particular TPPs. In such case, ASPSPs should ensure that any restriction of TPPs' access is done in compliance with the PSD2, including, where

[14] See footnote 3.

[15] See for example the responses to comments 82 and 85 in the feedback table on the final Guidelines, available at the link in footnote 4.

[16] See: https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4309

applicable, the requirements in Article 68(5) PSD2, which allows ASPSPs to deny an AISP/PISP access to a payment account where the ASPSPs has “objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account” by that AISP/PISP.

46. As regards access to corporate accounts, the EBA notes that the terms and conditions concluded by ASPSPs with the PSU (i.e. here: a legal entity) holding the respective account(s) may specify that only certain authorised users acting on behalf of the PSU can operate the corporate accounts. In the EBA’s view, ASPSPs should not impose additional checks when a user accesses the corporate accounts or initiates a payment from such accounts using the services of an AISP/PISP, compared to the checks applied when the same user directly accesses the said accounts or initiates a payment from such accounts.

Additional registrations

47. Some market participants reported cases where TPPs are required to go through additional registration processes at each ASPSP level in order to have access to the ASPSP’s interface, and queried whether such registration processes are an obstacle.

48. Article 32(3) RTS specifically mentions “requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of PSD2” as a potential obstacle.

49. The EBA acknowledges that some registration processes might be technically required to enable a secure communication with the ASPSP, without them necessarily amounting to an obstacle. For example, the implementation of the requirements in paragraph 16 above might require a pre-registration of the TPP’s app in order to enable a secure communication with the ASPSP’s authentication app. In the EBA’s view, such registration is not an obstacle if it is technically necessary to enable a secure communication with the ASPSP, is processed in a timely manner, and does not create unnecessary friction in the customer journey.

50. However, additional registrations required by ASPSPs for TPPs to be able to access the PSUs’ payment accounts, or the ASPSPs’ production interface, that go beyond what is technically necessary in order to ensure secure access to payment accounts under the conditions of the RTS, are an obstacle. For example, a requirement imposed by an ASPSP to TPPs to pre-register their contact details with the ASPSP in order for TPPs to have access to the ASPSP’s API is an obstacle. This being said, a registration process that is optional, or that is agreed between the ASPSP and TPPs, is not an obstacle.

51. Also, additional mandatory registration steps or processes with the ASPSP in order for the TPP to have access to the ASPSP’s production API, other than the identification of the TPP via an eIDAS certificate in accordance with Article 34 RTS, are an obstacle.

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

Done at Paris, 4 June 2020

[signed]

José Manuel Campa

Chairperson for the Board of Supervisors