EBA responses to issues XXI to XXVI raised by participants of the EBA Working Group on APIs under PSD2

Published on 14 August 2019

Disclaimer: The information contained in the table below is of an informational nature and has no binding force in law. Only the Court of Justice of the European Union can provide definitive interpretations of EU legislation. The information may factually reflect a given challenge faced by the industry, reiterate the European Banking Authority's views that have been previously published, reflect discussions that have been held on the practical implementation of legal requirements, or may include examples of industry practices. The information is also without prejudice to any future decisions made or views expressed by the European Banking Authority.

ID	Topic	Description	EBA Response
XXI	Machine-readability of the central register of the EBA under PSD2	Several participants in the EBA API WG have asked the EBA to publish a document that clarifies the data fields and properties used in the JSON file with the content of the central register of the EBA under PSD2. These participants argued that the publication of this document will allow all stakeholders to understand the JSON file more clearly.	The EBA agrees that clarifying the data fields of the machine-readable JSON file with the information contained on the central register of EBA under PSD2 will allow market participants better to interpret the information contained in the register. Therefore, on 5 August 2019, the EBA published a document with the specification of the data properties of the JSON file with the content of the central register of the EBA under PSD2, available on the right hand side of the above webpage.
XXII	Measurement of response times of the dedicated interface	Several API WG participants requested clarifications as to what should be included in the calculation of the key performance indicator (KPI) on response times under Guideline 2.3 of the EBA Guidelines on the exemption from the contingency mechanism. In particular, participants queried whether this calculation should include the time it takes to conduct SCA or the time it takes for the ASPSP to verify the authorisation/registration of third party-providers (TPPs).	As clarified in the Final Report on the EBA Guidelines on the conditions to benefit from an exemption from the contingency mechanism, the response time under Guideline 2.3 includes "the interval between the point in time when a request is received by the ASPSP from a PISP, AISP or CBPII and the point in time when all the information requested (or where relevant the yes/no confirmation) has been sent back by the ASPSP" (page 43 of the feedback table, comment 15). As further clarified in the feedback table on the Guidelines (page 44, comment 15), the response time includes the time it takes to check the authorisation/registration of TPPs, in particular the TPP's eIDAs certificate in accordance with

			Article 34(1) of the Delegated Regulation 2018/389 (the RTS). The question as to whether the time needed to conduct SCA should be included in the calculation of response times has been answered through Q&A 4661 published on 9 August 2019.
XXIII	Contingency mechanism in Art. 33(4) – Identification of TPPs through "guestbooks"	Some API-WG participants explained that they are exploring a number of solutions for identification of TPPs for the purpose of the contingency access in Art. 33(6) RTS that differ in complexity and, implicitly, costs required for their implementation. Some API WG participants queried whether one of the methods that they are exploring would be in line with the RTS. Under such method, TPPs would have to, first, register at a central registration point, referred to by the respective API WG participants as a "guestbook", by providing their PSD2 eIDAS certificate (i.e. a qualified certificate for website authentication) when registering in the guestbook, before accessing the ASPSP's systems. The actual access to the PSU accounts would then be a subsequent and separate step from this registration and the ASPSP would not be able to identify the TPP or check whether the TPP has performed the guestbook entry at the time when the TPP is accessing the ASPSPs' online channel. The participants who proposed this identification method acknowledged that it comes at the loss of precision with respect to logging of the actual access on the ASPSP's side, but pointed out that such method would be less costly than other identification methods explored by the industry. Participants queried as to whether the EBA considers this approach to be compliant with the RTS.	In accordance with Article 34(1) RTS, the identification of TPPs towards the ASPSP should be based on the use of qualified certificates for electronic seals (QSealCs) and/or qualified certificates for website authentication (QWACs) compliant with the Regulation (EU) No 910/2014 (eIDAS Regulation). Art. 33(5) RTS requires ASPSPs to ensure that TPPs can be identified when using the contingency mechanism in Art. 33(4) RTS. The same requirements regarding identification of TPPs with QSealCs/QWACs apply irrespective of whether the TPPs are accessing the PSUs' payment accounts via the dedicated interface or via the PSU interface(s) (as a primary access method under Art. 31 RTS or as a contingency access method under Art. 33(4) RTS). As clarified in paragraph 16 of the EBA Opinion on the use of eIDAS certificates under the RTS on SCA&CSC (EBA-Op-2018-7), "since the ASPSP is the party that should provide the interface and ensure the security of the communication session, it should be the party that chooses the type of certificate to use under Article 34(1) of the RTS". Concerning in particular the guestbook identification explored by some API WG participants, the EBA is of the view that such identification method does not meet the

			requirements in Art. 34(1) and 33(5) RTS, as it does not allow ASPSPs to rely on the eIDAS certificates for the identification of TPPs. In addition, such guestbook entry would not be compliant with the PSD2 because the ASPSP would not be able to check whether the TPP has identified itself at the time the access takes place. In this respect, Article 66(3)(d) of PSD2 provides that PISPs should identify themselves towards the ASPSP “every time a payment is initiated”. Similarly, Article 66(2)(c) PSD2 requires AISPs to identify themselves towards the ASPSP “for each communication session”. Finally, such guestbook registration would impose a condition for the identification of the TPPs that does not have any legal basis in PSD2 or the RTS.
XXIV	Contingency mechanism in Art. 33(4) RTS – Data that can be accessed	Several API WG participants requested clarifications as to whether ASPSPs need to make any changes to their existing customer interfaces for the purpose of the contingency mechanism in Art. 33(4) RTS. In particular, several API-WG participants queried whether ASPSPs must limit the data that TPPs can access through the PSU interface when using the contingency mechanism in Art. 33(4) RTS.	According to Article 33(5) RTS, for the purpose of the contingency mechanism in Art. 33(4) RTS, ASPSPs should ensure that TPPs “can be identified”, meaning that TPPs are able to identify themselves towards the ASPSP using eIDAS certificates in accordance with Art. 34(1) RTS, and that TPPs can rely on the authentication procedures provided by the ASPSP to its PSUs. The contingency mechanism should also enable TPPs to perform the actions in Art. 30(1) RTS, namely to: - enable AISPs to “communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions”; and - enable PISPs to “communicate securely to initiate a payment order from the payer's payment account and receive all information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction”.

			As regards the scope of data that can be accessed by TPPs through the contingency access in Art. 33(4) RTS, the PSD2 and the RTS do not provide any obligation for the ASPSP to limit the data that TPPs can see when accessing through the PSU interface, except for the requirement in Art. 36.1(a) RTS regarding the disclosure of sensitive payment data (detailed below). Articles 66 and 67 of PSD2 and Article 33(5) RTS place the responsibility on the TPPs, and not the ASPSPs, to ensure that the TPP does not access data for purposes other than for the provision of the service as requested by the PSU. The only situation where the RTS require ASPSPs to restrict access to certain data is the one referred to in Art. 36.1(a) RTS, according to which ASPSPs "shall provide [AISPs] with the same information from designated payment accounts [...] made available to the payment service user when directly requesting access to the account information, *provided that this information does not include sensitive payment data*" (emphasis added). "Sensitive payment data" is defined in Art. 4(32) PSD2 as "data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner an and the account number do not constitute sensitive payment data". The above is without prejudice to any other obligations that ASPSPs may have, for example under the EU General Data Protection Regulation 2016/679 (GDPR), to limit access to certain personal data of their customers.
XXV	Documentation of the	Several API-WG participants requested clarifications whether ASPSPs are required to document the contingency access in Art. 33(4), and if so, by when.	Article 33(1) RTS provides that "Account servicing payment service providers shall include, in the design of the dedicated

	contingency mechanism in Art. 33(4) RTS	TPPs expressed concerns that many ASPSPs have not yet documented how the contingency mechanism will be implemented and that they do not have visibility on how strong customer authentication (SCA) will be carried out by ASPSPs from 14 September where access is made through the contingency mechanism in Art. 33(4) RTS. Some TPPs raised concerns that this may lead to a disruption of TPPs services on 14 September 2019.	interface, a strategy and plans for contingency measures for the event that the interface does not perform in compliance with Article 32, that there is unplanned unavailability of the interface and that there is a systems breakdown”. Article 33(2) RTS provides that the “Contingency measures shall include communication plans to inform payment service providers making use of the dedicated interface of measures to restore the system and a description of the immediately available alternative options payment service providers may have during this time”. Furthermore, Art. 33(5) RTS provides, for the purposes of the contingency mechanism referred to in Article 33(4), that ASPSPs ensure that TPPs can be identified and can rely on the authentication procedures provided by the ASPSP to its PSUs. The RTS do not provide a deadline by which ASPSPs should document the access through the contingency mechanism. Nevertheless, in accordance with Art. 33(1) and (2) referred to above, ASPSPs shall set out a strategy and plans for the contingency measures and communications plans to inform TPPs of the “immediately available alternative options” through which they can continue providing their services while the API is restored. Such strategy and communication plans must be provided also in relation to the use of the contingency mechanism in Article 33(4) of the RTS, which is one of the contingency measures that ASPSPs are required to put in place. To this end, ASPSPs that do not receive an exemption in accordance with Art. 33(6), or whose exemption has been revoked by the national competent authority (NCAs) in accordance with Art. 33(7) RTS, should include in such strategy and communication plans a description of the contingency mechanism and of the

			authentication procedures on which TPPs can rely under Art. 33(5) RTS.
XXVI	Availability of, and reliance on, eIDAS certificates under Art. 34 RTS	Several API WG participants expressed their concerns about the difficulty in obtaining eIDAS certificates (QWACs and QSealCs) as referred to in Art. 34 RTS from qualified trust service providers (QTSPs). Some TPPs argued that because of this reason they could not test ASPSPs' production interfaces.	The EBA understands that one of the reasons for the delay and difficulty in the issuance of eIDAS certificates by QTSPs was uncertainty as to how to interpret the reference to "authorisation number" in Article 34(2) RTS. In response, the EBA already clarified in Q&A 4679 that the reference to "authorisation number" in Article 34(2) RTS includes "all forms of national identification numbers that are used by NCAs under PSD2 and allow the unequivocal identification of the payment service providers (PSPs) in the national registers under PSD2 and CRDIV as well as in the EBA PSD2 and credit institution registers". Nevertheless, in order to allow QTSPs better to interpret the information available on the EBA PSD2 and credit institution registers, the EBA published on 31 July 2019 several technical documents relevant for the EBA Opinion on the use of eIDAS certificates under the RTS on SCA&CSC (EBA-Op-2018-7), which are available on the right hand side of the above webpage. These include a document with the identification numbers used in the EBA registers that clarifies the types of national identification numbers used by each NCA in said registers. In addition, for the purpose of providing additional certainty to QTSPs in the process of issuing eIDAS PSD2 certificates the EBA also published on 31 July 2019 two additional documents with NCA abbreviations for inclusion in eIDAS certificates and the email addresses of CAs for the notification exchange with QTSPs. The latter document, which is in support of paragraph 32 of the EBA Opinion on the use of eIDAS certificates also aims at ensuring the timely revocation of eIDAS certificates after an authorisation of a TPP has been withdrawn by the respective

			NCA and is complementary to the response to issue XIII of the clarifications to the third set of issues raised by the EBA Working Group on APIs under PSD2, published on 26 April 2019 (pages 5-8).