EBA responses to issues XXXII to XXXVIII raised by participants of the EBA Working Group on APIs under PSD2

Published on 20 October 2021

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
XXXII	Downtime of dedicated interfaces	The submitter explained that some account servicing payment service providers (ASPSPs) inform third party providers (TPPs) about any planned or unplanned maintenance on their dedicated interfaces right before (e.g. less than 24 hours) the expected start of the maintenance and subsequent unavailability of the interface. The submitter explained that subsequently TPPs do not have sufficient time to prepare to switch to the interface made available to the payment service user (PSU) for the authentication and communication with the ASPSP. In addition, the submitter informed that ASPSPs announce planned or unplanned unavailability of their dedicated interfaces to TPPs by email, which does not allow TPPs to react quickly enough since the email may not get noticed by staff of TPPs. The submitter also explained that ASPSPs inform TPPs about the restoration of the availability of the dedicated interface by email, which may cause further delays in the provision of the services offered by TPPs. In order to address the issue, the submitter suggested that ASPSP shall inform TPPs of any	Article 32(1) of the RTS on SCA&CSC provides that ASPSP '*shall ensure that the dedicated interface offers at all times the same level of availability and performance, including support, as the interfaces made available to the payment service user for directly accessing its payment account online*'. Article 33(1) of the RTS on SCA&CSC provides that ASPSPs *'shall include, in the design of the dedicated 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) of the RTS on SCA&CSC further specifies 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*'. In accordance with the aforementioned Articles, and as part of the communication plans, ASPSPs shall inform TPPs about planned or unplanned unavailability of their dedicated and about the restoration of the dedicated interface at least at the same time the information is communicated in the interfaces made available to the PSUs for directly accessing their payment accounts online. The RTS on SCA&CSC, however, do not prescribe the time at which information about planned or unplanned unavailability and the restoration of the interface shall be communicated to the PSU. With regard to the channel used by ASPSPs to inform TPPs about any unavailability of the dedicated interface, the RTS on SCA&CSC also do not prescribe a specific channel to be

		planned maintenance on their dedicated interface as soon as possible and comparable to the time of announcement in the interface ASPSP make available to their PSUs. Another solution proposed by the submitter was for EBA to develop a central register where ASPSPs can communicate information about any upcoming maintenance of their dedicated interfaces. The majority of the other participants were not supportive of a solution based on a register since it is resource intensive.	used as part of the communication plans. Therefore, it is for each payment service provider to decide on the channel used for informing TPPs about any unavailability of their dedicated interface. Accordingly, ASPSPs are not prevented from using email for this purpose. In relation to the suggestion for the EBA to set up a central register/database where ASPSPs can communicate information about any upcoming maintenance of their dedicated interfaces, the EBA, in line with the views expressed by the majority of the API WG participants, is of the view that this proposal would introduce additional and unnecessary administrative burden for all stakeholders involved, namely ASPSPs that would need to submit the information, TPPs that would need to search for the information in the register and for EBA to set up and operate such a register. Furthermore, the EBA is of the view that under the current legal framework (PSD2 and the RTS on SCA&CSC), the EBA cannot require all ASPSPs that have implemented a dedicated interface to report additional indicators to those under Article 32 of PSD2 on the operation and performance of their interfaces. Such an obligation to ASPSPs would first require an assessment on whether it is proportionate or not, and in case it is, subsequently would require an amendment to the RTS on SCA&CSC. Finally, in accordance with Article 15 of PSD2, the EBA developed and operates a central register of payment institutions and electronic money institutions authorised within the EU. PSD2 has not conferred on the EBA to develop other registers or databases.
XXXIII	Payment status / rejection reasons	The submitter explained that ASPSPs often reject payments without specifying the reason in an error code or the payment status and that TPPs need to take proactive actions in order to understand the reason why the payment had been rejected. The submitter further explained that some ASPSPs reject payments after having previously informed a payment initiation service provider (PISP) that the payment has been initiated for execution. In the latter cases, the submitter argued that PISPs are not duly informed by the ASPSP. Finally, the submitter asked for EBA to set out the minimum set of error codes and payment status messages ASPSPs should send to TPPs.	Article 36(2) of the RTS on SCA&CSC prescribes that '*in case of an unexpected event or error occurring during the process of identification, authentication, or the exchange of the data elements, the account servicing payment service provider shall send a notification message to the payment initiation service provider or the account information service provider and the payment service provider issuing card-based payment instruments which explains the reason for the unexpected event or error.*' Accordingly, in case of an unexpected event or error during the process of identification, authentication, or the exchange of the data elements, ASPSPs are required to send a notification message to TPPs allowing the latter to understand clearly and unambiguously the specific reason for the unexpected event or error. In relation to the request from TPPs to receive a notification message on the reason for rejecting a payment transaction after the ASPSP has confirmed its initiation, it should be

		ASPSP representatives explained that the confirmation of the initiation of the transaction proves only that the payment was accepted for settlement and processing and does not ensure that the transaction will be executed and should, therefore, not be considered as a final payment status on the execution. This is because APSPS may detect fraudulent transactions during the execution stage.	noted that the unexpected events or errors under Article 36(2) of the RTS on SCA&CSC refer only to the process of identification, authentication, or the exchange of the data elements. Moreover, in line with Article 66(4)(b) of PSD2 and Article 36(1)(b) of the RTS on SCA&CSC, and as clarified in Q&A 4601, ASPSP are required to provide to PISPs all information on the initiation of the payment transaction and all information accessible to the ASPSP on the execution of the payment transaction immediately after the receipt of the payment order communicated by the PISP. This means that if the ASPSP is not aware immediately after the receipt of the payment order whether the payment will be executed or not, it is not required to provide such information to the PISP at a later stage. Finally, in relation to the proposal that the EBA should set out the minimum set of error codes and payment status messages that ASPSPs should send to TPPs, the EBA is of the view that these relate to implementations of the interfaces chosen by the ASPSPs, the specific events and errors that may occur, as well as the respective business models of TPPs. Relatedly, as explained in comment 67 of the Feedback table of the Guidelines on the conditions to benefit from an exemption from the contingency mechanism (EBA/GL/2018/07), '*the RTS do not impose any standardised error messages that ASPSPs should send to TPPs in accordance with Article 36(2) of the RTS. Therefore, the EBA is of the view that the GL cannot impose this either*'. Accordingly, it should be left out for the industry to set out the notification messages on the specific reason for any unexpected events or errors. Moreover, Article 36(2) of the RTS on SCA&CSC provides sufficient clarity on the content of these notification messages.
XXXIV	ASPSPs restricting access in case of embedded redirection	The submitter explained that the approach of 'embedded redirection' entails a TPP embedding the redirection domain of the ASPSP, with the PSU subsequently entering their credentials in the TPP domain instead of the ASPSP redirection domain and the TPP transmitting the credentials to the ASPSP in order to access the payment account information or to initiate a payment transaction. In the view of the submitter, this approach significantly improves the customer journey since the PSU does not leave the TPP domain, which in turn leads to fewer authentication steps, quicker	This issue has subsequently been submitted to the EBA as a question via the EBA's Q&A tool on the day of the publication of this document. Following its categorisation, the question will be published and answered in the Q&A tool.

		and less frictionless authentication journey for the PSU. The issue raised was that some ASPSP have not allowed the 'embedded redirection' and subsequently deny access to the payment account due to security concerns, which in the view of the submitter is not in line with Article 68(5) of PSD2 since the ASPSP does not have an objectively justifiable reason. The majority of the representatives of ASPSPs and API initiatives explained that the security concerns related to the fact that in this case, TPPs control the security credentials of PSUs and, therefore, ASPSPs cannot carry out properly their fraud monitoring mechanisms.	
XXXV	Scope of the bank offered consent	The submitter introduced the bank-offered consent model and explained that in the workflow, a TPP sends an access request without indicating specific payment accounts and, in some cases, the scope of the information to be accessed. The PSU, in turn, can select the payment accounts and the scope of the information to be accessed on the ASPSP's redirect page or on a mobile application (in case of a decoupled strong customer authentication (SCA) approach). The submitter further clarified that the approach they, as an ASPSP, have taken with the implementation of the Bank-offered consent is that the ASPSP's redirect screen would pre-populate all payment accounts and the full scope of the available account information with the possibility for the PSU to deselect specific payment accounts and/or specific account information. The submitter	This issue has subsequently been submitted to the EBA as a question via the EBA's Q&A tool on the day of the publication of this document. Following its categorisation, the question will be published and answered in the Q&A tool.

		suggested that such an approach should be followed in a harmonised manner across the EU because it gives the possibility for the PSU to define fully the consent in the ASPSP's domain. The TPP representatives raised concerns with the approach since they viewed it as an additional check by the ASPSP of the consent given from the PSU to the TPP and that it may lead to a change in the data to be accessed compared to the data agreed between the PSU and the TPP. Some TPP representatives were also concerned that ASPSPs may use language that does not reflect the intended service, which may subsequently confuse PSUs.	
XXXVI	Inability to initiate bulk payments via APIs	The submitter explained that the dedicated interfaces of ASPSPs in a particular country do not allow PSUs to initiate bulk payments for unregistered beneficiaries through a PISP. The submitter further explained that while registering beneficiaries for bulk payments can be done in the PSU direct interface, the PSU is not able to add a new beneficiary for bulk payments through a PISP.	This issue has subsequently been submitted to the EBA via the EBA's Q&A tool as Q&A 6236 and will be answered there.
XXXVII	Is EBICS in or out of PSD2 scope	The submitter asked whether the EBICS protocol falls within the scope of PSD2 and in particular whether SCA needs to be applied for initiating payment transactions and accessing payment account information. A few API WG participants informed that SCA is applied for initiating payment transactions but that the access to information is not online and thus not requiring the application of SCA.	This issue has subsequently been submitted to the EBA via the EBA's Q&A tool as Q&A 6235, with an amended wording, and will be answered there.
XXXVIII	90-day account	The submitter informed that account information service providers (AISPs) are losing a large part of their customers each time they are asked to	While the EBA disagrees with the solutions suggested by the participant, as they are legally not possible under the Directive, the EBA agrees that the application of the exemption under Article 10 of the RTS on SCA&CSC has led to undesirable outcomes for account

	access renewal SCA	reauthenticate due to the added friction in the customer journey caused by the authentication experience offered by ASPSPs, together with the fact that the SCA exemption under Article 10 of the RTS on SCA&CSC has not been applied consistently by ASPSPs prompting, at times, more frequent application of SCA in an AIS journey, including every time the PSU accesses its account online. The submitter informed these led to detrimental impact on AISPs' services in the cases where ASPSPs have implemented a redirection or a decoupled approach for SCA. The submitter suggested addressing the issue by clarifying that: ➢ SCA does not apply in the cases where the AISP, based on the PSU's explicit consent, accesses account information without the PSU active involvement; ➢ SCA for account access can be applied with the AISP directly.	information services, their providers, and their users. To address this issue, the EBA has, therefore, decided to make a targeted amendment on this particular aspect, which will be published for consultation later in 2021.