EBA responses to issues XIV to XX raised by participants of the EBA Working Group on APIs under PSD2

Published on 26 July 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
XIV.	Confirmation of payment execution	One participant queried whether account servicing payment service providers (ASPSPs) are required under Article 36(1)(b) of the RTS on SCA &CSC (the RTS) to provide information on the initiation and execution of the payment transaction, including updates, in order for a payment initiation service provider (PISP) to comply with Article 46(a) PSD2. The TPP argued that PISPs need to know the status of the payment execution after the initiation of the payment order in order to provide certainty to the merchant and the payment service user (PSU) whether the payment will complete. They highlighted that, the earlier the merchant knows a payment is rejected, the quicker it can offer alternative payment solutions to the PSU, thus avoiding abandoned carts and loss of revenue, and also that, without this confirmation, customers may incur penalty fees and excess interest if they do not know their payment has failed. On the other hand, ASPSPs argued that there is no legal requirement under either PSD2 or the RTS to provide such updates to PISPs, after the actual payment initiation, on the status of the payment order and that many ASPSPs do not even provide an explicit information regarding the successful settlement of a payment transaction to their own customers. They highlighted that Art. 66(4)(b) of PSD2 and Art. 36(1)(b) of the RTS requires them to provide all information on the initiation of the payment transaction and all information accessible to the ASPSP from a PISP "immediately after receipt of the payment	This question has been answered through the EBA's Q&A tool as Q&A 4601 published on 07 June 2019.

		order from the PISP" and that there is no legal requirement to provide further updates to PISPs beyond this. The discussions in the API WG also highlighted that some API initiative standards provide the functionality for ASPSPs to share updates on the payment status with PISPs as an optional functionality.	
XV	Biometrics and authentication on mobile apps	Several participants raised concerns that the APIs currently offered or being developed by many banks do not support app-to-app redirection or so-called decoupled authentication (which allows the customer to authenticate using a dedicated authentication application of the ASPSP, such as a banking app on a mobile phone) when the customer is using a TPP, although some of those banks allow their customers to authenticate via the ASPSP's mobile app or use biometrics to authenticate in the online channels of the ASPSP in order to access account information and/or initiate payments directly. These participants stressed that ASPSPs should allow AIS and PIS providers to rely on all the authentication procedure(s) provided by the ASPSP to its PSUs. In particular, they highlighted that ASPSPs supporting the use of biometrics in their mobile/online channels should also support authentication via biometrics in their dedicated interfaces. TPPs highlighted that this is essential in order to ensure a seamless customer experience and not to create obstacle to the provision of AIS and PIS.	In accordance with Article 97(2) of PSD2 and Article 30(2) of the RTS, ASPSPs should ensure that their dedicated interface does not prevent PISPs and AISPs from relying upon the authentication procedure(s) provided by the ASPSP to its PSUs. As clarified in paragraph 50 of the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04) and the Final report on the EBA Guidelines on the conditions to benefit from an exemption from the fall-back mechanism (EBA/GL/2018/07) (feedback table, page 68, comment 75 and page 75, comment 89), ASPSPs' dedicated interfaces should support all authentication methods made available by the ASPSP to its PSUs when an AISP or PISP is used. Accordingly, the method of access, or combination of methods that the dedicated interface should support, will depend on the authentication procedures that the ASPSP offers to its own PSUs, and whether security credentials are transmittable (such as a passwords) or not (such as biometrics). This means that, ASPSPs that have implemented a redirection approach and that enable their own PSUs to authenticate via the ASPSP's mobile app when the PSU directly accesses his/her account should also support app-to-app redirect when the customer uses a TPP. App-to-app redirection should allow the TPP to redirect a PSU from the TPP mobile application to the ASPSP's mobile application,

			installed on the PSU's device, where PSUs can then authenticate using the same credentials/methods as normally used for accessing their account directly. This should not involve additional steps than would be the case when the PSU authenticates with the ASPSP directly (such as being redirected first to the ASPSP's mobile website). Finally, ASPSPs that support authentication using biometrics in their direct customer channels should also support these authentication methods when the PSU is using a PIS or AIS provider. In such case, given that biometrics are not transmittable credentials, ASPSPs should support decoupled or app-to-app redirect to the ASPSP 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).
XVI	Access to non-payment account information	One API WG participant highlighted that, in many cases, TPPs will need to accommodate different access methods to access accounts data, depending on the type of account they are accessing (e.g. use APIs for accessing payment accounts data, and the customer interface for accessing non-payment accounts). The participant highlighted that it is very difficult for TPPs, in particular AIS providers, when accessing data from non-payment accounts using the customer interface, for example through screen-scraping, to ensure that they do not inadvertently access payment accounts data as well, given that TPPs may not be able to distinguish between accounts that are payment accounts and those that are non-payment accounts. The participant suggested that TPPs accessing non-payment account data via the customer interface should be permitted to also access payment account data subject to: - Identification of such accounts at summary level, without capturing transaction detail, where feasible;	The requirements in PSD2 and the RTS regarding access by TPPs to the customers' accounts data apply only in respect of payment accounts and do not cover other types of accounts. A payment account is defined in Article 4(12) of PSD2 as "an account held in the name of one or more payment service users which is used for the execution of payment transactions". The definition of payment accounts has been further clarified in the case-law of the European Court of Justice (ECJ) - see in particular the ECJ judgement from 4 October 2018, in Case C-191/17, available at: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-191/17. Although this ECJ judgement was rendered in respect of a savings account under Directive 2007/64/EC (PSD1), the principles it sets out are also applicable in the context of PSD2, given that the definition of 'payment accounts' under PSD2 has remained substantially the same as under PSD1. In line with the ECJ judgment, the

		- Deletion of payment data captured through this process (payment accounts data should not be processed beyond what is required to identify it). Said participant also suggested this could be further improved if ASPSPs would publish guidance on their test facilities documenting how TPPs can avoid capturing payment account data when using the customer interface. Several ASPSP participants of the API WG argued, however, that it is the TPPs' responsibility to ensure that the TPPs comply with the PSD2 and RTS requirements on access to payment accounts, and that ASPSPs have no legal obligation to share non-payment account data with third party providers, or to document how TPPs can avoid capturing PSD2 data sets when screen-scraping for non-payment accounts data. One API WG participant also noted that ASPSPs need to have a legal ground under the General Data Protection Regulation (GDPR) to be able to share non-payment account data with TPPs.	qualification of an account as a payment account will depend on the actual functionalities of that account. By contrast, its denomination on its own is not a determining criterion to determine whether or not the account is a payment account. From 14 September 2019, TPPs should access payment accounts data in accordance with the requirements set out in PSD2 and the RTS. Once the RTS apply, existing practices of third-party providers accessing the PSU data via the customer interface without identification (commonly referred to as 'screen scraping') will no longer be allowed for accessing payment accounts data. As highlighted in Article 66(3)(g) and 67(2)(f) PSD2, it is the obligation of the AISP/PISP to ensure that they do not 'use, access or store'data that is not necessary for performing the AIS/PIS requested by the payment service user; this obligation does not fall on the ASPSPs. Furthermore, both ASPSPs and TPPs are required to comply with their obligations under the EU data protection legislation (GDPR), which applies to all personal data they process.
XVII	Stress testing	One participant queried whether stress testing of ASPSPs' dedicated interfaces can be carried out in a testing environment with features very close to the real production environment, and whether this would be in line with the EBA Guidelines on the exemption from the contingency mechanism in Article 33(4) RTS. Said participant explained that stress testing is typically carried out in a testing environment with features very close to the production environment, rather than in the production environment itself, and that this is done for several reasons, including the fact that:	As set out in Guideline 4.1 of the EBA Guidelines on the conditions to benefit from an exemption from the fall-back mechanism (EBA/GL/2018/07), "For the purpose of the stress tests referred to in Article 32(2) of the RTS, the ASPSP should have in place processes to establish and assess how the dedicated interface performs when subjected to an extremely high number of requests from PISPs, AISPs and CBPIIs, in terms of the impact that such stresses have on the availability and performance of the dedicated interface and

		- Stress testing implies handling large volumes of requests from TPPs, and it is not easy to enable such volume of requests in the production environment without real users (and user's consent) behind those services; - Stress testing in the production environment could affect service levels already agreed with the PSU for other web interfaces and servers that use the same back-end production environment.	the defined service level targets". This can be achieved by carrying out stress tests in an environment having the same infrastructure and features as the dedicated interface in production, and does not need to involve real customers. Such approach is compliant with the requirements in the EBA Guidelines mentioned above, provided that the requirements set out in those Guidelines are met.
XVIII	Qualified eIDAS certificates for ASPSPs	One participant queried whether a credit institution in its role as TPP needs to include these roles in its eIDAS certificate under Article 34 of the RTS.	As clarified in paragraph 27 of the EBA Opinion on the use of eIDAS certificates under the RTS on SCA&CSC (EBA-Op-2018-7), "credit institutions can provide all the payment services referred to in Annex I to PSD2 as part of their authorisation under Directive 2013/36/EU without being authorised for each of the payment services they provide. Therefore, credit institutions that act in their capacity as a third party provider (whether as an AISP, a PISP and/or a CBPII) should be assigned the three roles 'payment initiation', 'account information' and 'issuing of card-based payment instruments' at the same time". Paragraph 28 of said Opinion further clarifies that "in the scenario where the PSP acts in its capacity as an ASPSP and offers to PSUs accounts that are accessible online, said PSP should be assigned the role 'account servicing'". This has also been clarified in Q&A 4413.
XIX	4 times per day access by AISPs	One API WG participant was of the view that the limit in Article 36(5) RTS of four times per day access by AISPs for unattended access should not apply to ASPSPs' dedicated interfaces. The participant stressed that this limitation significantly limits the utility for PSUs to use AIS providers and the ability of AISPs to provide timely alerts to PSUs, and that it may compel PSUs to centralise their activities on their ASPSP instead, due to the superior user experience available this way. The participant also argued that it is impractical to expect AIS providers to have contractual arrangements with every ASPSP in order to be	According to Article 36(5) RTS, "Account information service providers shall be able to access information from designated payment accounts and associated payment transactions held by account servicing payment service providers for the purposes of performing the account information service in either of the following circumstances: (a) whenever the payment service user is actively requesting such information;

		able to access account data without the customer's involvement beyond the 4 times a day limit in Article 36(5) RTS. In this participant's view, the limitation of 4 times per day access in Article 36(5) RTS was intended to ensure that ASPSPs' interfaces used by PSUs are not overloaded with TPP requests and should not apply to ASPSPs' dedicated interfaces. The participant suggested this issue may be solved if ASPSPs would offer a "push notification" mechanism, where changes to payment accounts or new payment transactions can be pushed out to AISPs that have registered a PSU's interest in receiving such notifications, filtered if the case based on the PSU's requirements.	(b) where the payment service user does not actively request such information, no more than four times in a 24-hour period, unless a higher frequency is agreed between the account information service provider and the account servicing payment service provider, with the payment service user's consent". As clarified in paragraph 28 of the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04) and Q&A 4210, this Article 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 the PSU 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. AISPs and ASPSPs may contractually agree for the AISP to access the account without the customer's involvement at a higher frequency, or for the ASPSP to push information to the AISP, with the PSU's consent. However, this is not a mandatory requirement under the PSD2 or the RTS. The limitation in Article 36(5) RTS applies irrespective of the access interface the ASPSP has chosen to implement in accordance with Article 31 RTS, i.e. whether it is a dedicated interface or an adapted customer interface.
XX	Sharing of payment account number with PISPs	One participant was of the view that it is necessary in order to mitigate fraud risks for ASPSPs to share the payment account IBAN/number with PISPs. This participant argued that the risk of fraud is particularly high in case of merchant refunds through a PISP, as the refund process could potentially be used by fraudsters to receive the money in a different account. The participant explained that, in case of a refund request, merchants typically refund the money to the customer through the same method the customer has	Regarding the sharing of the account number by ASPSPs with PISPs, the Q&A 4188 clarifies that ASPSPs are only required to provide or make available to PISPs the information necessary for the provision of the PIS. The same Q&A clarifies that, since it is always the PSU that specifies the account from which the transaction is to be initiated, there is no need for the ASPSP to provide or make

		used to make the original payment, and that in order to receive a refund the customer only needs the order reference, the item or it's description and address details. The participant argued that it is relatively easy for a fraudster to obtain these details and then claim refund to be sent to another account. To mitigate such risk, the participant suggested that PISPs could obtain their customers' consent to receive account details and that the ASPSP could, based on that consent, provide details to the PISP of the account selected by the customer to authorise the payment.	available to the PIS provider a list with all the account numbers of the PSU "as long as this would not create obstacles for the provision of PIS as per Article 32(3) of the [RTS]". In relation to this, the EBA has also clarified in the Final Report on the EBA Guidelines on the conditions to benefit from an exemption from the contingency mechanism (feedback table, page 71, comment 80) that "if the PSU does not select the account in the PISP's domain and the account is not known in advance, [...] the ASPSP may ask the customer to select the account on the ASPSP's domain, as part of the authentication step, before the customer is redirected back to the PISP's interface, without this representing an obstacle". In the case of a merchant refund, the PSU would be the beneficiary of that refund. Refunds of a transaction initiated through a PISP may or not imply the use of an PISP. In such case it is for the merchant and the PSU to agree on the method through which the refund is to be made and the payment account to which the refund will be credited.