EBA responses to issues XXVII to XXXI raised by participants of the EBA Working Group on APIs under PSD2

Published on 30 July 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
XXVII	Authentication with electronic signature required by ASPSPs	A participant of the API WG requested a clarification on whether account servicing payment service providers (ASPSPs) can request the use of electronic signature when a payment service user (PSU) accesses account information through an account information service provider (AISP) instead of, or at times in addition to, the usual strong customer authentication (SCA) procedure the ASPSP has chosen to use when the PSU accesses their account online directly with the ASPSP. The same participant also noted that, when an electronic signature is being applied, the PSU is asked to sign a generic (and at times lengthy) text, instead of the verification of the identity of the PSU. The use of electronic signatures was also seen as preventing AISPs to make use of authentication procedures that lead to good customer journeys, such as those relying on biometric authentication.	Article 30(2) of the Commission Delegated Regulation (EU) 2018/389 (RTS on SCA&CSC) provides that 'for the purposes of authentication of the payment service user the interface… shall allow account information service providers and payment initiation service providers to rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user.' The EBA has further clarified related aspects to this provision in the Opinion on the implementation of the RTS on SCA&CSC (EBA-Op-2018-04) and the Opinion on obstacles (EBA/OP/2020/10), in particular that all authentication procedures provided from the ASPSP to the PSU need to be supported by the ASPSP's dedicated interface when an AISP or a payment initiation service provider (PISP) is used. With regard to the point on the use of biometrics for authentication in an account information service (AIS) journey, issue XV from the fourth set of clarifications to the EBA working group on APIs under PSD2 published in July 2019 as well as paragraph 12 of the Opinion on obstacles, have already clarified that ASPSPs that enable their PSUs to authenticate using biometrics when directly accessing their payment accounts or initiating a payment should 'enable their PSUs to use biometrics to authenticate with the ASPSP in a PIS or AIS journey.' Since ASPSPs should not impose a more burdensome SCA procedure in an AIS journey compared to that used when the PSU accesses their account online directly with the ASPSP, requesting authentication of the PSU in an AIS journey through an electronic signature when a different SCA procedure is requested in the direct channel, will not be compliant with the requirements of the RTS on SCA&CSC and would constitute an obstacle to the provision of AIS under Article 32(3) of the RTS on SCA&CSC.

			With regard to the application of the electronic signature in an AIS journey in addition to the SCA procedure that is also used in the direct channel, it would constitute an obstacle to the provision of AIS, including when the electronic signature is used for the creation of the 90-days token for the exemption under Article 10 of the RTS. This is in line with paragraph 23 of the Opinion on obstacles, which clarified that '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.'
XXVIII	Biometrics and authentication on mobile apps (2)	A participant of the API WG shared security concerns related to the use of biometrics in an app-to-app redirection scenario. In particular, their concerns were that there is a dependence on the operating system (OS) and fraudsters may exploit vulnerabilities to gain access to the transferred data at application and/or OS level due to standard technical implementation of the app-to-app redirection by ASPSPs that requires the mobile application to register a particular service on the OS of the device. The same participant suggested for the EBA to identify common technological standards for a harmonized solution at EU level. A few other participants of the API WG were of the view that there have not been many fraud cases and that it is challenging and complex to address this concern.	Article 30(2) of the RTS on SCA&CSC provides that 'for the purposes of authentication of the payment service user the interface… shall allow account information service providers and payment initiation service providers to rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user.' As clarified in the fourth set of clarifications to the EBA working group on APIs under PSD2 published in July 2019 (issue XV) and paragraph 12 of the Opinion on obstaces, ASPSPs that enable their PSUs to authenticate using biometrics when directly accessing their payment accounts or initiating a payment should 'enable their PSUs to use biometrics to authenticate with the ASPSP in a PIS or AIS journey'. Paragraph 49 of the same Opinion clarified that ASPSPs can set up registration processes that are technically required to enable a secure communication with the ASPSP, without them necessarily amounting to an obstacle. Therefore, the EBA has provided sufficient clarity on the application of Article 30(2) of the RTS on SCA&CSC in relation to the issue at hand, and no additional such clarifications are needed in response to this issue. In line with the approach taken during the development of the RTS on SCA&CSC to keep technological and business model neutrality and to facilitate innovation, the EBA does not see merit in introducing common technological standards for a harmonised solution at EU level as proposed by the participant of the API WG. The EBA is of the view that the harmonised and consistent application of the legal requirements on access to payment accounts has been

			facilitiated by the large number of clarifications provided with different EBA Opinions, the Guidelines on the conditions to benefit from an exemption from the contingency mechanism under the RTS on SCA&CSC (EBA/GL/2018/07), and a large number of answers to questions posed on the EBA Q&A tool.
XXIX	Social engineering fraud	One participant of the API WG observed that the fraud rate of payment transactions initiated by PISPs are much higher compared to transactions initiated directly with the ASPSP. In their view, PSUs are not properly informed by PISPs on fraud cases, social engineering fraud in particular, or their fraud monitoring does not work properly. In the view of the participant, PSUs approach ASPSPs when the transaction has already been executed and ASPSPs cannot do anything. At the same time ASPSPs' fraud monitoring cannot detect these fraudulent transactions due to the absence of PSU-related information (e.g. IP-address, location, etc.) PISPs participating in the API WG were of the view that warning measures undermine trust in their service and that cases where ASPSPs include such warnings in the redirection flow will penalise PISPs and challenge the legitimate use of PIS.	Social engineering fraud is a type of fraud different from all other types of payment fraud, in that the fraudster does not directly compromise a payment tansaction or a financial institution. Rather, the fraudster exploits human error or cognitive biases to manipulate a user into performing an action that is not in the user's interest, including the disclosure of the PSU's personalised security credentials, to commit fraud. This type of fraud is not easily addressed by the fraud prevention requirements introduced in PSD2. However, a number of requirements have been developed that signficantly reduce the risk of social engineering fraud. Given that PISPs are authorised payment service providers, they are required to comply with these requirements. In particular, PISPs that are payment and electronic money instutions must comply with the requirement of Article 5(1)(j) of PSD2, which specifies that as part of the authorisation procedure payment institutions (and electronic money institutions) shall submit 'a security policy document, including a detailed risk assessment in relation to its payment services and a description of security control and mitigation measures taken to adequately protect payment service users against the risks identified, including fraud…'. Furthermore, Article 2 of the RTS on SCA&CSC requires from all PSPs to have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions. In addition, they are required to comply with the requirements set out in the following EBA Guidelines: • The EBA Guidelines under PSD2 on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers (EBA/GL/2017/09), in particular 'the organisational measures and tools for the prevention of fraud' and 'security policy document containing… a detailed risk assessment of the payment service(s) the applicant intends to provide, which should include risks of fraud and the security controls and mitigation measures taken to adequately protect payment service users against the risks identified'. • The EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), in particular Guideline 3.8, which, inter alia, prescribes that 'PSPs should establish and implement

			processes to enhance PSUs' awareness of the security risks linked to the payment services by providing PSUs with assistance and guidance' and that 'the assistance and guidance offered to PSUs should be updated in the light of new threats and vulnerabilities, and changes should be communicated to the PSU'. • The EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions under the AMLD (EBA/GL/2021/02) (Risk factor Guidelines), including the steps to be taken 'to prevent impersonation or identity fraud' and, where relevant, applying identity fraud checks to ensure that the customer is who they claim to be. In line with the referred Guidelines, all PSPs, including PISPs, should introduce tools and measures to prevent fraud, including by informing their PSUs on the risk of social engineering fraud and other applicable types of fraud. Furthermore, the above requirements do not prevent ASPSPs from introducing a warning measure to PSUs in relation to social engineering fraud in a redirection flow, under the condition that ASPSPs have introduced the same warning measure when the PSU initiates a payment transaction directly with the ASPSP, as otherwise the additional warning measure would constitute an obstacle and, therefore, a breach of law. This follows from the clarification provided in paragraphs 7 and 15 of the Opinion on Obstacles because by implementing an additional warning measure, the ASPSP will introduce an additional step and friction to the PIS journey and may undermine the trustworthiness of PISPs, including by using discouraging language that could directly or indirectly dissuade the PSUs from using the services of a PISP. In addition, Article 36(4) of the RTS on SCA&CSC prescribes that PISPs shall provide ASPSPs 'with the same information as requested from the payment service user when initiating the payment transaction directly'. Therefore, provided that applicable legal requirements are being met, including by obtaining the consent of the PSU, PISPs shall provide information that would allow ASPSPs to apply the security measures they have put in place to mitigate the risk of known fraud cases, including social engineering fraud.
XXX	Ability of PISPs to refuse a	A few TPP participants of the API WG asked whether the name of the account holder and	Article 66(4)(b) of PSD2 and Article 36(1)(b) of the RTS on SCA&CSC prescribe that ASPSPs shall provide or make available to PISPs all information on the initiation of the payment transaction

	payer's request to initiate a payment transaction	the IBAN can be shared with PISPs before the initiation of the payment transaction in order to prevent attempts to carry out fraud (including by the payer) before the initiation of the payment transaction. ASPSPs and API initiatives participating in the API WG were of the view that sufficient clarity has been provided with published Q&As and the EBA Opinion on obstacles.	and all information accessible to the ASPSP regarding the execution of the payment transaction immediately after the receipt of the payment order. Therefore, ASPSPs are not legally required to provide information to PISPs before the initiation of the payment transaction. PISPs can obtain the relevant account number (IBAN) from the PSU themselves or by relying on an AIS license. Q&A 4188 clarified that there is no need for the ASPSP to provide or make available to the PISP a list with all the account numbers of the payment service user and the associated currencies, as long as this would not create obstacles for the provision of PIS as per Article 32(3) of the RTS on SCA&CSC. In addition, in line with the clarifications in paragraph 34 of the Opinion on obstacles and Q&A 4854, ASPSPs should not reject the requests received from PISPs in a redirection or decoupled approach, simply because the PISP has not transmitted to the ASPSP the relevant account details. Q&A 4081 further clarified that ASPSPs shall, immediately after receipt of the payment order, provide the name of the payer (the PSU) to the PISP via the dedicated interface if the name is included in the information on the initiation and execution of the payment transaction provided or made available to the PSU when the transaction is initiated directly by the latter. In addition, to address the fraud concern, PISPs, being obliged entities under the AMLD and therefore required to comply with the 'know your customer' requirements, should also make every effort to comply with the requirements set out in the Risk factor Guidelines and adopt security policy and tools for the prevention of fraud based on their risk models.
XXXI	Complexity in the ASPSP authentication process	Several participants of the API WG considered ASPSP authentication processes in a TPP journey more complex compared to the authentication process when the PSU accesses their payment account online or initiates a payment transaction directly with the ASPSP. In their view, the TPP journey had extra steps, additional security measures and vague and ambiguous messages.	As clarified in the EBA Opinion on obstacles, the authentication procedure with the ASPSP as part of an AIS/PIS journey should not create unnecessary friction or include unnecessary steps, including multiple SCAs, or require the PSU to provide unnecessary information compared to the equivalent authentication procedure offered to PSUs when directly accessing their payment accounts or initiating a payment with the ASPSP. The EBA deemed such unnecessary steps or information required as obstacles under Article 32(3) RTS on SCA&CSC. Further, in order to ensure that obstacles are removed by ASPSPs, the EBA issued an Opinion on supervisory actions to ensure the removal of obstacles to account access under PSD2 (EBA/Op/2021/02) where the EBA set out its expectations on the supervisiory actions to be taken

		In the view of these participants, additional metrics should be introduced to compare the authentication process in a TPP journey and in the ASPSP direct channel and published frequently by ASPSPs. In their view, these metrics can include authentication success rate, duration of the authentication, and type and ratio of errors that occur. An alternative suggestion of metrics put forward by some participants was for the metrics also to measure the number of authentication steps.	by CAs and the deadlines for such actions. In line with said Opinion, to ensure a consistent application and supervision of relevant requirements of the PSD2 and the RTS on SCA&CSC, the EBA has been monitoring the way in which the supervisory actions have been taken into account, so as to contribute to a level playing field across the EU. The EBA is of the view that the above clarifications and actions for now address the issue on the complexity in the ASPSPs' authentication processes. With regard to the suggestion to publish metrics, Article 32(1), (2) and (4) of the RTS on SCA&CSC prescribes 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', that ASPSPs 'shall define transparent key performance indicators and service level targets, at least as stringent as those set for the interface used by their payment service users both in terms of availability and of data provided' and that ASPSPs 'shall publish on their website quarterly statistics on the availability and performance of the dedicated interface and of the interface used by its payment service users'. The EBA further set out requirements for the key indicators on availability and performance in Guideline 2 of the EBA Guidelines on the conditions to benefit from an exemption from the contingency mechanism under the RTS on SCA&CSC (EBA/GL/2018/07). In relation to the above, there is no legal basis to request the suggested additional indicators. Moreover, it will be difficult and timely to set these indicators up in a way that will be consistently understood and applied by the industry, as well as to measure and compare them in a meaningful way. Further, as also stressed by many of the other participants of the API WG, it will be resource intensive for ASPSPs to report and publish these additional indicators, while at the same time focus of ASPSPs should be kept on removal of any remaining obstacles as specified above. Given the above, and in view of the additional reporting burden any new indicators would create for the 5000+ ASPSPs in the EU, the EBA sees no strong case to develop such requirements at this point in time but is prepared to reconsider this in 2022, if necessary.