EBA responses to issues VIII to XIII raised by participants of the EBA Working Group on APIs under PSD2

Published on 26 April 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
XIII.	Portability of 'wide usage' data between Member States	One participant queried whether the data collected on the 3 months' wide usage period referred to in Article 33(6) of the RTS on SCA&CSC, showing wide usage of the dedicated interface and produced in one Member State by an ASPSP belonging to an ASPSP Group, can be used as evidence to support the 'widely used' condition in another Member State for a separate ASPSP belonging to the same Group, on the condition that both entities employ the same dedicated interface.	This question has been answered through the EBA's Q&A tool as Q&A 4638 published on 26 April 2019.
IX.	Passporting and eIDAS certificates	One participant queried whether ASPSPs have to check whether TPPs are authorized to operate in their member state under the free provision of services or the right of establishment, considering that eIDAS PSD2 certificates do not contain any passporting information.	This question has been answered through the EBA's Q&A tool as Q&A 4432 published on 26 April 2019.

X.	Use of eIDAS certificates during the wide' usage period prior to 14.09.2019	Another issue raised by participants was whether the use of eIDAS certificates is mandatory during the 3-months 'wide usage' period specified in Article 33(6) (c) of the RTS on SCA&CSC for accessing payment accounts via APIs prior to the application date of the RTS, i.e. 14 September 2019.	This question has been answered through the EBA's Q&A tool as Q&A 4630 published on 26 April 2019.
XI.	The use by TPPs of agents and outsourcees for accessing payment accounts data	Some participants raised a number of queries regarding the use by third party providers (TPPs) providing account information or payment initiation services of agents or technical service providers (TSPs) for accessing the customers' payment accounts held with an account servicing payment service provider (ASPSP). In particular, these participants queried whether the ASPSP is required to check only the principal TPP identified in the certificate. In their view, since agents and TSPs are not payment service providers (PSPs) and do not have PSD2 eIDAS certificates, the ASPSP is only required to identify the TPP mentioned in the eIDAS certificate. These participants also argued that, even in the case where the agent used by the TPP is regulated and appears in a national register, there is no legal	In accordance with Article 34 of the Commission Delegated Regulation (EU) 2018/389 (RTS on SCA&CSC), TPPs must identify themselves towards the ASPSP for accessing the customers' payment accounts data, by using an eIDAS certificate. As clarified in paragraph 21 of the EBA Opinion on the use of eIDAS certificates under the RTS on SCA&CSC (EBA-Op-2018-7), if an eIDAS certificate is presented by an agent or TSP acting on behalf of a TPP, the certificate should unequivocally identify the principal TPP on behalf of which the agent or TSP is acting. The question whether the name of the agent or TSP should also be included in the eIDAS certificate, and whether the ASPSP is required to identify the agent or only the principal TPP mentioned in the certificate, has been answered in the Q&A 4507 published on 26 April 2019 Furthermore, as clarified in the EBA Opinion referred to above, the TPP remains fully responsible and liable for the acts of its agents and outsource providers as well as for the revocation and updating of the eIDAS certificates used by them. In addition, TPPs should ensure that they comply with their own information and disclosure requirements towards the PSU as set out in Title III of PSD2. The EBA also notes that Article 19(6) of the PSD2 explicitly requires payment institutions to ensure that agents acting on their behalf inform PSUs of this fact. It is therefore not the ASPSP's responsibility to inform the PSU that the TPP is acting through an agent.

		obligation for the ASPSP to check the existence or status of such an agent. These participants added that some API initiatives, such as STET, have developed an approach through which TPPs can declare that the request comes from an agent, but explained that under the STET standards this as an option for the TPP, not a requirement. They further argued that, for the purpose of transparency and more clarity for the payment service user (PSU), TPPs using agents to access payment accounts data should be encouraged to declare, when possible through the API, what agent is acting on their behalf. Furthermore, these participants argued that, if the API allows for the transport of such information, the ASPSP should be encouraged to provide this information to the PSU. Finally, they argued that, since the TPP is liable for its own agents, there should be an automated refund mechanism in case the agent is fraudulent or has been withdrawn from the register, and that, in the absence of such a mechanism, the ASPSP should be allowed to warn the PSU	With regard to the approaches apparently developed by some API initiatives for the identification of agents, the EBA reiterates that, while these approaches may indeed facilitate the identification of the agent requesting access on behalf of the TPP, ASPSPs are only legally required to identify the TPP, not its agent as well. As regards the ability for the ASPSP to warn the PSU and/or block access the EBA notes that, in accordance with Article 68(5) of PSD2, an ASPSP is entitled to block access to payment accounts data to TPPs for "objectively justified and duly evidenced reasons" that should only be related to "unauthorised or fraudulent access to the payment account" by the TPP. In such event, in accordance with Article 68(6) of PSD2, the ASPSP should immediately report the incident to the NCA, specifying the reasons for taking such an action. PSD2 does not restrict the ASPSP from informing the PSU that it has conducted such block, and the reason for this action.

		that the agent is suspected of fraudulent behaviour or withdrawn from a national register, and/or block the exchange.	
XII.	'Widely used' and 'design to the satisfaction of the TPPs' conditions	One participant was of the view that the EBA has watered down the requirements for TPPs' involvement in the process of granting an exemption for an API as stated in the SCA&CSC RTS, in particular the conditions in Art. 33(6) (b) and (c) of the RTS on SCA&CSC regarding the design and testing to the satisfaction of TPPs and the wide usage conditions. This participant was concerned that this may leave the door open for the mandatory use of inadequate APIs.	As described in the final report on the Guidelines on the conditions to benefit from an exemption from the fall-back mechanism (EBA/GL/2018/07), the EBA received the same comments when it was consulting on the draft Guidelines in autumn 2018, agreed that the concerns were valid, and introduced a number of changes to address these concerns before it published the final Guidelines. In particular, the EBA enhanced the way in which TPPs can be involved in the exemption process. For example, Guideline 6 requires ASPSPs to provide to their national competent authority (NCA) the feedback they received from TPPs that took part in the testing and explain how they have addressed the issues reported by TPPs. The Guidelines also require ASPSPs to provide information to the NCA on their engagement with TPPs, and clarify that, in order to meet the 'design' condition, ASPSPs need to prove that their API complies with all the legal requirements on access to data in PSD2 and the RTS, including the requirement not to create 'obstacles' to the provision of account information and payment initiation services as provided in Article 33(2) RTS on SCA&CSC. The Guidelines also clarify that the 'wide usage' condition should be assessed taking into account the number of TPPs that have used the ASPSP's production interface for offering services to their customers, the number of successful requests sent by TPPs via the dedicated interface during the 3-months wide usage period, but also other factors, such as the steps that the ASPSP has taken to achieve 'wide usage'. The EBA strongly encourages TPPs to test the APIs being developed by ASPSPs and to provide feedback to ASPSPs on any issues they encounter with the test or production interfaces, so that ASPSPs can address those issues and develop high-performing and customer focussed APIs.

XIII.	ASPSPs relying on eIDAS certificates	A number of market participants raised concerns that there could be a potential mismatch between the information contained in the eIDAS PSD2 certificate and the information contained on the EBA and national registers, in the case of a revoked authorisation in particular. They highlighted the risk of ASPSPs sharing information with parties that are no longer authorised by NCAs, in case their eIDAS certificate is still active. These market participants also expressed concerns that ASPSPs cannot rely on the information contained on the EBA and national registers for identification of TPPs after the date of application of the RTS on SCA&CSC in addition to the use of eIDAS certificates. They also querried whether there is a potential time gap between the authorisation being withdrawn and the update of the authorisation status in the national (and EBA) registers, as well as in industry directories. In the view of these participants, NCAs should communicate the revocation of the authorisation of a TPP to the qualified trust service provider (QTSP) that has issued the respective eIDAS PSD2	In accordance with Article 34 of the RTS on SCA&CSC, for the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 or for website authentication as referred to in Article 3(39) of that Regulation (eIDAS Regulation). This means that, when a TPP identifies itself towards the ASPSP via an eIDAS PSD2 certificate, the ASPSP shall grant access to the TPP to the specified account. ASPSPs are not legally required to rely on any other means for the purpose of identification of TPPs. However, ASPSPs may choose to carry out additional checks of the authorisation/ registration status of TPPs in the respective EBA and/or national registers, provided that, in doing so, ASPSPs do not create obstacles to the provision of payment initiation and/or account information services, as required in Article 32(3) of the RTS. For example, as stated in Guideline 5.1(b) of the EBA Guidelines on the exemption to the fallback mechanism (EBA/GL/2018/07), if such checks were to create delays or friction in the customer journey that would directly or indirectualy dissuade customers from using the services of TPPs, this would represent an obstacle prohibited by Article 32(3) of the RTS. In relation to the update of the public information in case of a withdrawn authorisation, Article 13(3) of PSD2 requires NCAs to make each withdrawal of authorisation public, including in their national registers and the EBA PSD2 Register. Depending on national administrative law and practices, the precise steps of the withdrawal process will differ between Member States. However, the EBA would assume that national authorities will update their respective national register at the time when the withdrawal takes legal effect. With regard to the publication of such updates on the EBA Register, and in line with the requirements set out in Article 15(2) of PSD2 and in the Commission Delegated Regulation (EU) 2019/411 (the RTS on the

		certificate (and who can also revoke said certificate), in line with paragraph 32 of the EBA Opinion on the use of eIDAS certificates, on a mandatory basis. One industry participant also querried whether there is a reasonable time for providing access to account data to a TPP the authorisation of which has been withdrawn fom the registers but has its eIDAS certificate still active.	EBA Register), NCAs are required to do so without delay, but at the latest by the end of the day when the respective change in the national register has been made. With regard to the publication of the information in industry directories, neither the EBA nor NCAs are required to update any such directories and therefore do not take any responsibility for the accuracy of any information provided by them. With regard to the suggestion for NCAs to be required to take a proactive role in the revocation of the eIDAS PSD2 certificates, it should be noted that, in line with the requirements of the eIDAS Regulation, paragraph 31 of the EBA Opinion on the use of eIDAS certificates under the RTS on SCA&CSC (EBA-Op-2018-7) clarifies that "qualified trust service providers are responsible for checking the validity of the information in the eIDAS certificates at the time of issuance of the certificate, and both QTSPs and PSPs are responsible for ensuring the information is kept up to date and for revoking the certificates". In order to address concerns raised by the industry at the time the Opinion was prepared, paragraph 32 of the same EBA Opinion goes a step further, by establishing a process whereby NCAs can request the revocation of an eIDAS certificate when they have withdrawn the authorisation of a PSP, but have not been informed by either the QTSP or the PSP that the certificate of the latter has been revoked. NCAs are not required to follow this process under any EU law, an EBA legal instrument, national law or a national regulation. Rather, the process constitutes a mechanism, to be adhered to on a voluntary basis, for NCAs to notify the relevant QTSP that the authorisation status or the scope of activities of a particular PSP has changed, thus allowing the QTSPs to perform the checks they are required to undertake under the eIDAS Regulation in order to revoke the certificate. It should be noted that QTSPs remain responsible on their side to check the trustworthiness of the certificates they issue under the eIDAS regulation. PSPs, in turn, remain similarly responsible for the reliability of the certificates they use. The

			process of the email notifications envisaged in paragraph 32 of the EBA Opinion does not change the attribution of liability for an incorrect certificate. However, as participants of the EBA Working Group have continued to express concerns about the lack of transparency as to which NCAs will or will not follow this process, the EBA is providing in the Annex overleaf the indications that NCAs have given to the EBA as of 26 April 2019. It should be noted that the indications provided in the Annex do not guarantee that an NCA will request a revocation of an eIDAS certificate in every single case, as the specifics of a particular withdrawal of authorisation may require the NCA to take a different action. Finally, it should be noted that, in accordance with Article 37(1) of PSD2, Member States shall prohibit natural or legal persons that are neither PSPs nor explicitly excluded from the scope of PSD2 from providing payment services. Therefore requesting access to a payment account without an authorisation is a breach of PSD2 and the respective national legislation transposing the Directive.

Annex to the EBA response to issue XIII: List of NCAs that will follow the process for requesting the revocation of an eIDAS certificate when considered necessary, as set out in paragraph 32 of the EBA Opinion (EBA-OP-2018-7).

EU MS	Name of Authority	NCA follows process?
Austria	Austria Financial Market Authority	**Yes**
Belgium	National Bank of Belgium	**Yes**
Bulgaria	Bulgarian National Bank	**Yes**
Croatia	Croatian National Bank	**Yes**
Cyprus	Central Bank of Cyprus	**No view expressed**
Czech	Czech National Bank	**No**
Denmark	Danish Financial Supervisory Authority	**No view expressed**
Estonia	Estonia Financial Supervisory Authority	**No view expressed**
Finland	Finnish Financial Supervisory Authority	**Yes**
France	Prudential Supervisory and Resolution Authority	**No**
Germany	Federal Financial Supervisory Authority	**No**
Greece	Bank of Greece	**Yes**
Hungary	Central Bank of Hungary	**No view expressed**
Ireland	Central Bank of Ireland	**No**

EU MS	Name of Authority	NCA follows process?
Italy	Bank of Italy	**No view expressed**
Latvia	Financial and Capital Markets Commission	**Yes**
Lithuania	Bank of Lithuania	**Yes**
Luxembourg	Commission for the Supervision of Financial Sector	**Yes**
Malta	Malta Financial Services Authority	**Yes**
Netherlands	The Netherlands Bank	**Yes**
Poland	Polish Financial Supervision Authority	**Yes**
Portugal	Bank of Portugal	**Yes**
Romania	National Bank of Romania	**No view expressed**
Slovakia	National Bank of Slovakia	**Yes**
Slovenia	Bank of Slovenia	**Yes**
Spain	Bank of Spain	**Yes**
Sweden	Swedish Financial Supervision Authority	**Yes**
UK	Financial Conduct Authority	**Yes**