[**X**] Public – [ ] Internal Use – [ ] Confidential – [ ] Strictest Confidence
Distribution: General Public

API EVALUATION GROUP (EG)
RECOMMENDED FUNCTIONALITIES (PSD2/RTS)

1. Introduction

This document provides the API EG's view of where the market is at the time of publication and offers guidance to the market as per the scope and mandate of the API EG. Any relevant legal clarification under PSD2/RTS will be provided by or through the EBA. Ultimately, the national competent authorities (NCAs) will be responsible for assessing API implementations by individual ASPSP firms as part of their Dedicated Interface.

The views in this document represent the consensus agreement of API EG members. Where consensus has not been possible the views are clearly attributed and represent the opinions of that constituency only.

This document describes the recommended functionalities for APIs to achieve alignment to the PSD2, the RTS on SCA and SC and the EBA Opinion and to ensure good market facing outcomes and may be updated from time to time as necessary. Information is presented in tabular form describing; each individual recommended functionality (column 3); the support for each item required by the API specifications being developed by market facing API initiatives (column 4); and how the requirements relate to the ASPSP API dedicated interface (column 5). Views of the API EG members relative to the market facing considerations are also set out for each item as appropriate (column 6). The coverage and support for the recommended functionalities by the API initiatives in their specifications is set out in column 7 (colour coded: Green: supported by 4 initiatives; Yellow: supported by 2 or 3 initiatives; Orange: supported by 1 initiative or less) based on their input without further analysis by the API EG.

Please also note that a limited number of functionalities are subject to further clarification via the EBA. These are clearly marked in column 5 as "In the process of clarification by the EBA".

(N.B. Views expressed in the document do not necessarily reflect the views of the EBA or the European Commission)

2. Recommended functionalities

1. EBA Opinion Table 1 Main requirements	**2.Relevant articles**	**3. Recommended Functionality description**	**4. Common recommendation to be supported by API initiatives to achieve cross market consistency and harmonisation between specs (y = Yes should be supported)**	**5. Functionalities specific to ASPSPs seeking to meet the conditions for an exemption (Y = Yes should be implemented as explicitly legally required and as such to meet the conditions for an exemption / N = Not explicitly required to meet the conditions for an exemption but relevant to good market facing outcomes**	**6. Market facing commentary to inform considerations for implementing a good API for customers (specific comments attributed to ECSAs = European Credit Sector Associations (EBF, ESBG, EACB), BEUC = the European Consumer Organisation, TPPs = AISP and PISP providers, Retailers = EuroCommerce and Ecommerce Europe)**	**7. Coverage of recommended functionalities (RF) by API Initiatives (Berlin Group / NISP, Open Banking UK, STET, Polish API Initiative) (Note: number indicates how many out of a maximum of 4 API initiatives support the individual functionality based on their input to the API EG)**
Enabling CBPIIs, AISPs and PISPs to access the necessary data from payment accounts accessible online	Articles 66(4)(b)(c), 66 and 67 PSD2 Article 30 RTS Opinion 37-39 Opinion 23-26	**1**. Should enable the ASPSP to support AIS, PIS and CBPII for all payment accounts accessible online, regardless whether the account is an individual private account, a private joint account, a corporate account or any other payment account.	Y	Y		**4**

		2. Should support ASPSPs to: (a) immediately after receipt of the payment order from a PISP, provide or make available all information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction to the PISP.	Y	Y	Exact interpretation of all information on initiation accessible to the ASPSP is unclear. Certain types of data may be legally sensitive, such as suspected money laundering. Pertinent point is information on whether the payment will be executed.	**4**
		(b) immediately after receipt of the payment order, provide PISPs with the same 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.	Y	Y		**4**
		(c) upon request, immediately provide PISPs with a confirmation in a simple 'yes' or 'no' format, whether the amount necessary for the execution of a payment transaction is available* on the payment account of the payer.	Y	Y	*Available balance as defined in the EBA Opinion. **ECSAs:** There are circumstances where an ASPSP will not be able to provide a "yes/no" confirmation. This is the case when the payment may be checked manually by the ASPSP. If no "yes/no" answer can be provided by the ASPSP on the availability of funds, please refer to recommended functionality (RF) #3 (below) which will apply. **TPPs/Retailers**: Assumption is that no SCA is required for such a request.	**3**
		(d) provide or make available to the PISP a confirmation from the ASPSP that the payment will be executed.	Y	N	Not required by PSD2/RTS but can be provided under market facing agreement. Agreements could take any shape and form and be agreed bi-laterally, multi-laterally, nationally, x-community. These agreements would be formed in law outside PSD2 RTS respecting appropriate legal frameworks. This functionality would not apply to CBPII. **ECSAs:** A "confirmation that the payment will be executed" would be equal to a "payment guarantee", which is out of scope since that would be in the commercial space. A payment guarantee can of course be obtained by the PISP under a market facing agreement with the ASPSP. In the case of instant payments (e.g. SCT Inst) this distinction will become less relevant since a few seconds after initiation of a payment the PISP will know whether it was executed or not. The payment is separate from the service. **Retailers**: Confirmation of payment execution is a mandatory requirement for retailers in order to proceed with the delivery of goods or services. **TPPs:** Confirmation that payment will be executed would allow the PISP to notify the merchant immediately about certainty of funds.	**2**
		(e) prior to initiation of the payment, provide or make available to the PISP the IBANs (or equivalents) and currencies as available to the PSU for all payment accounts.	Y	In the process of clarification by the EBA	**ECSAs:** In a redirect scenario the information as described is typically not pushed by the ASPSP to the PISP. In this scenario the PSU is redirected to his internet/mobile banking environment, where the PSU authenticates himself and is presented with all payment accounts, balances and currencies. Here the PSU chooses from which account the payment is to be initiated, and after successful initiation (through authorisation via SCA) the PSU is directed back to the PISP (or, more likely, to the web merchant). This can be done in other ways as well, but this is the most common method. **TPPs & Retailers**: Such data should always be supplied to the TPP and the negative impact of serving this data up through a redirection only is discussed in RF# 32 and RF#33.	**2**
		(f) provide or make available to the PISP and to the AISP the name of the PSU (payer / AISP user).	Y	In the process of clarification by the EBA	**ECSAs:** Most of the ASPSPs have interpreted the name of the PSU as information not needed to be provided to the TPPs as it is not needed to initiate a payment or to use an account information service. The payer name is a data field the PISP or AISP should have obtained from the PSU before initiating a payment or from offering an account information service. There are assumptions made about the legal framework formed between PISP or AISP and the PSU relevant to obtaining this data. **Retailers**: PISP should send and receive rich data to/from the ASPSP to enable a SEPA payment instrument initiation for fraud risk mitigation. **TPPs:** Scenarios exist today in the live market where the TPP customer is the merchant and not the PSU directly.	**2** **support AISP not PISP**

		(g) provide or make available to the PISP the current balance of the payment account prior and/or after the initiation of the payment in case such balance is shown to the PSU directly.	Y	In the process of clarification by the EBA	As a general principle if information is provided by the ASPSP to the PSU then the ASPSP also needs to provide it to the TPP (PISP) via the API. **BEUC:** The PISP should not see the balance of the PSU. **ECSAs:** The available new balance **after** the payment has been initiated is by definition not part of the information that has to be provided to the PISP to allow him to **initiate** the payment. It may be of interest to the PISP, but if so, it has to be obtained as part of an AIS service. This may be different though, if the new balance after initiation is shown immediately after initiation as part of the payment initiation flow offered by the ASPSP to the PSU. **TPPs:** The provision of balance to help inform the customer when they're making a payment is a key part of the user experience. This could be relevant in an e-commerce scenario when the customer is trying to transact, and the customer needs to know how much money they have. Equally if a customer has multiple payment accounts with the same institution, the balance will be a key data point in helping them select from which account they'd like to transact.	**1**
		3. In the event that the ASPSP does not have a system that enables it to adequately respond to the yes / no confirmation request sent by the provider initiating the payment, it must provide the PISP with the necessary information required to assess whether there will be sufficient funds available at the time of execution of the payment.	Y	Y Conditional, depending on the ASPSP being able to provide a "yes/no" confirmation If the ASPSP cannot provide the "yes/no" answer it shall provide the data as specified in the EBA Opinion.	The data to be specified is detailed in the EBA Opinion. **ECSAs:** To note that providing additional data prior to a payment initiation may slow down the customer experience. The expectation is that the PISP will have obtained the consent of the PSU to share the relevant data on available balance. **TPPs:** In the absence of a reliable yes/no confirmation of the actual available balance, it is essential to obtain the necessary account data for scoring the risk of non-execution and then only initiate payments, which are sufficiently likely to get executed as well.	**2**
		4. Should provide data granularity in terms of data elements and time range covered (e.g. account statement data for a particular account over a certain amount of time) to ensure that there is an efficient way to access the appropriate data as per the PSU consent. Data minimisation principles apply.	Y	In the process of clarification by the EBA	Expectation towards the API initiatives is clear however further investigation is needed in relation to the implementation of this functionality by the ASPSPs in a way that is compliant with PSD2 and GDPR (e.g. ASPSPs cannot provide 3 years data if the TPP is only asking for 3 months). How much data is provided will vary according to the requirement to ensure equivalence (non-discrimination) between what is available to the PSU via their ASPSP online interface compared to the API interface. **ECSAs:** This recommendation should be based on the functions in the ASPSP environment to structure the data: there is no pick and choose menu for TPPs to choose from. Banks will make available relatively fixed data sets, depending on how they operate towards their clients at the moment and based on the privacy by default/by design principle. **TPPs**: It has to be up to the TPP to access only the data elements that are relevant and not more than that – so it can have a consent in place with the PSU that is not "broader" than what it has to be. It cannot be assumed that an ASPSP ex ante knows all potential "use cases", i.e. that innovation cannot happen, and as such provides certain pre-defined "batches" of data to fit them. Access to only specific data elements rather than predefined sets is also required due to GDPR data minimisation.	**3**
		5. Should provide access to the trusted beneficiary list to the AISP.	Y	In the process of clarification by the EBA	Trusted beneficiary list is considered to be the list of beneficiaries that have been authenticated such that a payment can be initiated without SCA where normally SCA would be required. The list, if provided by an ASPSP, should be made available to the AISP on the basis that this is something that the PSU can see currently via the ASPSP online interface. **ECSAs:** The list of trusted beneficiaries (LOTB) is a list that may be offered by the ASPSP to the PSU. Such list contains the names of beneficiaries which are known and may have received payments from the PSU previously, based on which the beneficiary can be "trusted". Adding beneficiaries to the LOTB requires SCA, and, most probably, removing a beneficiary from the LOTB would require SCA too. This trust, i.e. the certainty that the beneficiary is a bona fide party and would thus pose less risk, would allow the ASPSP to use, at its own discretion, an exemption from the SCA obligation. However, first, not all ASPSPs offer a LOTB. Second, adding and removing beneficiaries to the LOTB is a separate process from payment initiation, although it is conceivable that an ASPSP asks the PSU if it wants to add the beneficiary to the LOTB in the payment initiation process flow. Third, the LOTB is most likely not visible to the PSU during payment initiation, since the LOTB is a list that runs in the background. Fourth, this list can also contain sensitive information data both from customer point of view (beneficiaries with aliases being given by payer that are not for public consumption) and from transaction risk analysis/fraud point of view. In any case, there is no logic for the AISP to see the LOTB since it is only of relevance in the context of PIS, more specifically only relevant to the ASPSPs to decide whether or not to apply SCA. In the absence of market facing agreements, the PSU uses the credentials supplied by the ASPSP to perform SCA, and it is the ASPSP that decides on the application of an SCA exemption. Understandably, in order to allow for a smooth customer journey, the AISP/PISP may wish to suggest the ASPSP not to apply SCA and use an exemption, of course always within the mandate of the law. However, this would need a market facing agreement since further clarification between ASPSP and AISP/PISP is required how such suggestion would work, how it should be made and what the legal consequences would be. Further, under a market facing agreement, ASPSP and PISP can for example agree to include the messages "add to beneficiary list" and "the explicit consent of the PSU to add this specific payee to the beneficiary list" to their dedicated interface after which the ASPSP will add this beneficiary to the LOTB after proper due diligence.	**2**
		6. Should Provide access to the trusted beneficiary list to the PISP.	Y	In the process of clarification by the EBA		**0**

		Should allow for the payee for a PISP-initiated payment to be added to the trusted beneficiary list as part of the PIS flow.	Y	N		**1**
		Should enable the PISP to push information or suggest additions to the beneficiary list.	Y	N	Under market facing agreements **BEUC**: Does not support the idea that the PISP would see the trusted beneficiary list but does agree that with appropriate PSU authorisation the PISP could add to the trusted beneficiary list. **ECSAs**: The list of trusted beneficiaries (LOTB) is a list that may be offered by the ASPSP to the PSU. Such list contains the names of beneficiaries which are known and may have received payments from the PSU previously, based on which the beneficiary can be "trusted". Adding beneficiaries to the LOTB requires SCA, and, most probably, removing a beneficiary from the LOTB would require SCA too. This trust, i.e. the certainty that the beneficiary is a bona fide party and would thus pose less risk, would allow the ASPSP to use, at its own discretion, an exemption from the SCA obligation. However, first, not all ASPSPs offer a LOTB. Second, adding and removing beneficiaries to the LOTB is a separate process from payment initiation, although it is conceivable that an ASPSP asks the PSU if it wants to add the beneficiary to the LOTB in the payment initiation process flow. Third, the LOTB is most likely not visible to the PSU during payment initiation, since the LOTB is a list that runs in the background. Fourth, this list can also contain sensitive information data both from customer point of view (beneficiaries with aliases being given by payer that are not for public consumption) and from transaction risk analysis/fraud point of view. In any case, there is no logic for the AISP to see the LOTB since it is only of relevant in the context of PIS, more specifically only relevant to the ASPSPs to decide whether or not apply SCA. In the absence of market facing agreements, the PSU uses the credentials supplied by the ASPSP to perform SCA, and it is the ASPSP that decides on the application of an SCA exemption. Understandably, in order to allow for a smooth customer journey, the AISP/PISP may wish to suggest the ASPSP not to apply SCA and use an exemption, of course always within the mandate of the law. However, this would need a market facing agreement since further clarification between ASPSP and AIS/PISP is required how such suggestion would work, how it should be made and what the legal consequences would be. Further, under a market facing agreement, ASPSP and PISP can for example agree to include the messages "add to beneficiary list" and "the explicit consent of the PSU to add this specific payee to the beneficiary list" to their dedicated interface after which the ASPSP will add this beneficiary to the LOTB after proper due diligence **Retailers**: Firstly, merchants and their PISPs should be allowed to transmit the intention of the payer to add the merchant into their Trusted Beneficiary list. Therefore, the merchant will be able to communicate the exact Payee name and Trade/Brand name or any alias to be added in the Trusted Beneficiary list allowing the Payer to confirm the addition using the correct Beneficiary name, avoiding any potential issue with wrong spelling or wrong identification of the trusted beneficiary. Secondly, retailers would like to receive the information that the customer payment has been executed using the exemption of trusted beneficiary and to propose in the future a more convenient and seamless customer experience where feasible. **TPPs:** User journey would be improved if instead of having to log out of a TPP session and log in manually into the ASPSP to add a trusted beneficiary that benefits from SCA exemptions, the PSU could make such addition directly in the TPP session. PSU expectation would be that they can add a beneficiary to their list when making a payment to that beneficiary under the same SCA.	**0**
Conforming to (widely used) standard(s) of communication issued by international or European standardisation organisations	Article 30(3) RTS	**7.** Should conform to (widely used) standard(s) of communication issued by international or European standardisation organisations.	Y	Y		**4**
		8. Should not require the AISP or PISP to use specific tools or software when using the API.	Y	Y	Should not require the TPP to implement proprietary software of a given ASPSP or API initiative.	**4**
Allowing the payment service user (PSU) to authorise and consent to a payment transaction via a PISP	Article 64(2), 66 (3) PSD2 Article 30(1)(c) RTS Opinion 13 and 22-29	**9.** Should enable the ASPSP to support a PISP to initiate all types of payments in scope of PSD2 that a PSU can initiate in its ASPSP online / digital channels (regardless of the PSU being an individual or a legal entity).	Y	Y	A wide range of payment types will be in scope where a spec designed for wide adoption of markets must also enable all payments relevant to those markets to which the spec will apply (e.g. Sweden, United Kingdom).	**4**

		10. Allow the AISP and PISP to manage PSU consent without involvement of the ASPSP.	Y	Y	PSU consent means PSU consent provided to the PISP/AISP. **BEUC:** The informed consent is the most important dimension of the trust in open banking. A tick in a box saying that the consumer accepts terms and conditions of a document he will never read is not at all an informed, explicit and specific consent. The authentication does not mean the consumer has consented. The authentication does not allow the consumer's bank to know exactly what the consumer has given his agreement to. The consumer consent has to be handled completely independently of the authentication In the current situation the bank does not know exactly what the consumer has given his consent to. Is it access by the TPP to the account balance or to all the payments transactions? Access to past payments or also payments scheduled? There is a risk that some consumers have not understood what they have agreed to. Some consumers may want to be sure that they will never give a right to third parties to access their bank account. To allow that, consumers should have the right to instruct their bank not to accept the sharing of their data with third parties. The consumer needs to know to whom he has given access to his financial data. This information provided in a table (or dashboard in the UK open banking) should be provided by each bank. **ECSAs:** To note that it is essential for some customers to get an overview of TPPs that they are using and to which they have given a consent. This is a basic service expected by PSUs to be available which should be able to be provided by the ASPSP. This requires that the ASPSP should be able to receive the PSU consent from the TPP which the ASPSP has no legal right to obtain. **TPPs:** Per PSD2 the customer has the right to use AIS/PIS and ASPSPs must not block such provision other than for very specific reasons outlined in the legislation. Further, any suggestion that a TPP is not able to request consent per applicable legislation is wholly unfounded.	**4**
		11. Allow the transmission of the PSU consent from the PISP and AISP to the ASPSP.	Y	N	Under market facing agreement some ASPSPs might like to obtain this information from the TPP, e.g. in order to compose and display a list of all third-parties with which the user has interacted **BEUC:** The informed consent is the most important dimension of the trust in open banking. A tick in a box saying that the consumer accepts terms and conditions of a document he will never read is not at all an informed, explicit and specific consent. The authentication does not mean the consumer has consented. The authentication does not allow the consumer's bank to know exactly what the consumer has given his agreement to. The consumer consent has to be handled completely independently of the authentication In the current situation the bank does not know exactly what the consumer has given his consent to. Is it access by the TPP to the account balance or to all the payments transactions? Access to past payments or also payments scheduled? There is a risk that some consumers have not understood what they have agreed to. Some consumers may want to be sure that they will never give a right to third parties to access their bank account. To allow that, consumers should have the right to instruct their bank not to accept the sharing of their data with third parties. At least for AISP, the transmission of the consent to the ASPSP should be automatic. The consumer needs to know to whom he has given access to his financial data. This information provided in a table (or dashboard in the UK open banking) should be provided by each bank **ECSAs**: The above requires that the ASPSP should be able to receive the PSU consent from the TPP. **TPPs:** It must be clearly understood that according to RF#11 above, sharing PSU consent with ASPSPs can only be an optional, voluntary act and therefore not mandatory.	**4**
		12. Should enable the ASPSP to support a "pure" PIS journey, with a single SCA, whereby the PISP provides the ASPSP with: - the payer IBAN; - the payment scheme to be used; - the creditor name and IBAN (Account Number and routing identifier where applicable); - a transaction reference; - the payment amount, and - the currency of the payment, based on which the single SCA (dynamic linking) is	Y	Y	There may be variances in SCA steps between one-leg out and intra EU transactions. **ECSAs:** This is dependent on specific ASPSPs prerequisites and different market standards. This RF can be enabled on the assumption that there will have been prior steps between the ASPSP and the PISP to enable the exchange of consent token or other means of identification of the PSU. **Retailers**: Retailers believe that the payment context and related exemption type/SCA request must be added. For example, merchant and/or PISP are the only one that can securely indicate if a payment initiation is a contactless or remote low value, if the transaction is a recurring or installment with the first transaction being authorised (customer present) and the subsequent transactions with the customer not present, or if a SCA is required due to the POS environment or value. **TPPs:** No preceding SCA or consent token is needed according to PSD2/RTS and would constitute unnecessary and burdensome steps in the customer journey.	**4**

		triggered.				
		13. Should allow the PSU to set up and stop a standing order through the PISP and the ASPSP to be informed accordingly.	Y	Y	It is logical that the PSU can not only set up but also stop standing orders through the API. The PSU can also stop them directly in the online / mobile channel of the ASPSP. Two different scenarios to be distinguished in relation to standing orders. The standing order from the PSU rests with the PISP and PISP initiates payments according to the instruction, or the PISP provides to the ASPSP the data for the ASPSP to establish a standing instruction and the ASPSP initiates the payments not the PISP. Both scenarios are considered valid but will have different PSU outcomes. **ECSAs:** A PISP can only stop those payment orders that were set up through that PISP. The PISP does not have a reference to (i.e. is not aware of) other standing orders. Focus is only on standing orders and not on recurring card payments as the latter is dealt with by the merchants' acquirer. This notwithstanding, the API needs to fully support the CBPIIs as per Article 65 PSD2.	**3**
		15. Should allow the PSU to initiate and revoke a "future dated payment" through the PISP.	Y	Y	**ECSAs:** PISP can only revoke those future-dated orders that were set up through that PISP. The PISP does not have a reference to (i.e. is not aware of) other future-dated orders. The PSU can also revoke them directly in the online / mobile channel of the ASPSP.	**3**
		16. Should not allow the PSU to revoke a one-time only (not future dated) initiated payment transaction.	Y	Y	A repetition of PSD2 Art 80. Certainty of execution of the payment allows for earlier notification to Payee.	**3**
Enabling PISPs and AISPs to ensure that, when they transmit the personalised security credentials issued by the ASPSP, they do so through safe and efficient channels. Enabling a secure data exchange between the ASPSP and the PISP, AISP and CBPII, mitigating the risk of any misdirection of communication to other parties. Allowing traceability	Articles 66(3)(b) and 67(2)(b) PSD2 Articles 28, 29 and 35 RTS	**17**. Should allow identification by AISPs/PISPs/CBPIIs to ASPSPs.	Y	Y		**4**
		18. Should allow identification by ASPSPs to AISPs/PISPs/CBPIIs using eIDAS qualified certificates.	Y	N	The ASPSP is not required to use eIDAS if it is not undertaking a PSD2 role (i.e. AISP/PISP/CBPII).	**4**
		19. Should support that secure encryption is applied between the communicating parties (AISP, PISP, CBPII and ASPSP) throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.	Y	Y		**4**
		20. Should support communication sessions between the AISP, PISP or CBPII and the ASPSP to be uniquely and unambiguously identified for each operation.	Y	Y		**3**
Allowing 90-day reauthentication for AISPs	Article 10(2)(b) RTS Opinion 40-47	**21.** Should enable the ASPSP to support an AIS journey where the PSU goes through SCA using the ASPSP issued credentials during initial consent and subsequent renewal after 90 days would be carried out in such a way as to not to burden the PSU	Y	In the process of clarification by the EBA	**ECSAs:** The ASPSP view is that it is always the ASPSP SCA that will be used unless something else has been agreed as part of a market facing agreement. Indeed, the ASPSP is responsible towards its client both for not providing data that should not be leaked and for not making payments that should not be made and thus needs to keep SCA in its own hands. A delegation of SCA to a third party would constitute the outsourcing of an important function and would require an agreement with the parties to whom this function is outsourced. As both the TPP (and to a lesser extend the PSU) are aware of the last time SCA was performed, the TPP should be able to advise the PSU well in advance of the expiry of the consent reminding the PSU to renew the consent (at a moment convenient to the PSU). One could also state that it increases the burden for ASPSPs (that make use of this SCA exemption) and PSUs, because it implements a different customer flow than via the online channel (where the ASPSPs credentials will be used at least every 90 days and likely much more frequently). **TPPs:** PSUs having to do SCA for each ASPSP payment accounts connected to AISP every 90 days means that when a PSU connects 3 ASPSP to an AISP, they will have to	**3 (API EG considers this would benefit from further investigation as to the extent this RF is supported by the three API initiatives.)**

		[providing PSU's explicit consent is obtained every 90 days by the AISP].			do 3 SCA every 90 days to access his accounts through the AISP plus a further three times if he still wants to access his accounts directly from the ASPSP. And furthermore, if the SCA is performed via a "redirect" the AISP does not have control over the user experience of the SCA process at all (implying an unacceptable obstacle to the provision of AIS). For each ASPSP aggregated by an AISP, its AIS services (ex. Alert services to avoid overdrafts) will not be able to continue until the PSU performs the SCA. PSU will likely complain to the AISP because he is not respecting its commitment to inform about a risk of overdraft (in the above example). Benchmark: Current market practices of some banks include the request to the PSUs to change their passwords after a certain number of connections or a certain elapsed time since the password was last changed. In those cases, the PSU has to reconnect his bank to the AISP each time the password is changed. This is before the RTS or even PSD2 entering into force, and it looks like a smoother process than what we can expect from what is currently defined for SCA in some API Initiatives. In the current scenario, the practical result is that the PSU attrition rate for PSUs with accounts on the banks with such procedures is three times higher than the attrition rate for PSUs with other banks. Whereas SCA is done on a daily basis by AISPs for both kind of banks in parallel anyway (So PSU consent is renewed). It means that if the AISP can't manage the full experience of the consent renewal every 90 days, it will at the minimum translate the higher attrition rate to all users. The worst case will be the PSUs that have more than one bank connected to the AISP, because they will be required to perform several SCAs, one for each bank connected to the AISP. As a result, SCA managed by ASPSP for consent renewal every 90 days directly with the PSU, represents a huge obstacle for that renewal to actually happen. Rather, following the initial SCA performed by the PSU towards the ASPSP, subsequent SCAs should be enabled to be done through the AISP. Either being performed by the AISP on behalf of the PSU or using AISP-issued credentials.	
		22. Should enable a technical solution to support communication between an ASPSP and an AISP, PISP or CBPII regarding who does SCA.	Y	In the process of clarification by the EBA (i.e. dependent on EBA clarification of point 24)	This is a pre-requirement of RF #21. **ECSAs:** The ASPSP view is that it is always the ASPSP SCA that will be used unless something else has been agreed as part of a market facing agreement. Indeed, the ASPSP is responsible towards its client both for not providing data that should not be leaked and for not making payments that should not be made and thus needs to keep SCA in its own hands. A delegation of SCA to a third party would constitute the outsourcing of an important function and would require an agreement with the parties to whom this function is outsourced. As both the TPP (and to a lesser extend the PSU) are aware of the last time SCA was performed, the TPP should be able to advise the PSU well in advance of the expiry of the consent reminding the PSU to renew the consent (at a moment convenient to the PSU). One could also state that it increases the burden for ASPSPs (that make use of this SCA exemption) and PSUs, because it implements a different customer flow than via the online channel (where the ASPSPs credentials will be used every 90 days). **TPPs:** Allowing the PSU to renew consent, using SCA methods of the AISP rather than the ASPSP, after every 90 days after the initial consent with the ASPSP. This would reduce the burden for customers. Without this the impact on the AIS market could be significant because of the number of consents the AISP needs to go through.	1
Enabling the ASPSPs and AISPs to count the number of access requests during a given period	Article 36(5) RTS Opinion 28	**23.** Should enable AISPs access AIS-regulated information 4 times a day where the customer does not actively request such information.	Y	Y	It is unclear how this (i.e. 4 times a day) is measured and by whom. In some scenarios this information will only be presented to the TPP and not the ASPSP. If the user agrees access this is equivalent to 'actively requesting'. Unclear about the practical use of long-lived consent by the customer with the AISP.	3
		24. Should enable more frequent access than 4 times a day whenever the customer is actively requesting such information.	Y	Y		4
		25. Should require that when an agreement is cancelled by the consumer to the ASPSP (his/her bank) or the TPP, the party which has received the cancellation should inform the other party.	Y	N	The consumer should be able to cancel any specific agreement formed with a third party at any time. **TPPs**: Consent given to the TPP should be cancelled with the TPP. If SCA is not performed every 90 days, such consent in any event is withdrawn automatically. Allowing the ASPSP to revoke access to PIS/AIS introduces significant competition concerns and is in violation of Article 68 PSD2.	3
		26. Should enable ASPSPs to push data updates to AISPs in real-time as the changes are applied.	Y	N	Under market facing agreement (TPPs disagree that this always has to be under market facing agreement due to the non-discrimination principle.) **ECSAs**: First and foremost, it should be noted that this functionality cannot be provided by TPPs in the current screen scraping environment, and that this functionality also cannot be provided under the fall-back option. Second, not all ASPSPs offer this functionality, and third, out of those ASPSPs that offer such notifications, these are considered by some ASPSPs as a Value-Added Service and are offered to PSUs under an agreement and PSUs are charged for this. As such, ASPSPs consider this functionality, if present, as a value-added service and as such a market facing agreement is required to provide this service. **TPPs**: It allows a level playing field of services and the respect of the non-discrimination principle of PSD2 and RTS between ASPSP interfaces and AISP interfaces. For example, when a transaction is done, some banks are already sending a message in real time to the PSU to inform about this transaction. The PSU should have the same frequency of updated data and pushed data on ASPSPs interfaces AND on AISPs interfaces. Every time data is updated and / or pushed to ASPSP interfaces, it should be updated and / or pushed to AISP through API. If it is not the case, AISP interfaces will be discriminated in terms of services regarding ASPSP interfaces. As a result, API Initiatives should at least push updated data to AISP at the same frequency than what is done on ASPSP interfaces.	2
2Allowing a	Article	**27.** Should support the	Y appropriate open	Y	Opportunity to establish stronger coordination between API EG and API Initiatives to maximise consistency between specs.	4

change control process	30(4) RTS	ASPSP in the API change control procedure and governance.	and transparent governance for the API initiative should be defined. Including for example change control, versioning, decision making etc.			🟩
Allowing error messages explaining the reason for the unexpected event or error	Article 36(2) RTS	**28.** Should support related error messaging from the ASPSP to the AISP, PISP and CBPII.	Y	Y	It would be highly recommended to have standardised error codes.	**4**
Supporting access via technology service providers on behalf of authorised actors	Article 19(6) PSD2	**29**. Should support connection by technology service providers (technical services provided by a non-regulated entity acting on behalf of a regulated entity) using eIDAS certificate.	Y	Y, in the instance that the Technical Service Provider is involved	Certificate of the regulated entity (or certificate which specifies "acting on behalf of"). The ASPSP has to be able to identify the authorised entity. **ECSAs:** The "Y" in the ASPSP column is conditional on the condition that the ASPSP will be presented with the certificate of the regulated entity (or certificate which specifies "acting on behalf of"). The ASPSP has to be able to identify the authorised entity.	**4**
Allowing AISPs and PISPs to rely on all authentication procedures issued by the ASPSP to its customers	Article 97(5) PSD2 Article 30(2) and 32(3) RTS Opinion 50	**30.** Should allow the AISP or PISP to rely on all authentication procedures, including the use of personalised security credentials, issued by the ASPSP to the PSU where applicable.	Y	Y	Range of credentials has to be supported such as passwords, biometrics etc. **ECSAs**: … subject to technical compatibility between credentials and channels, e.g. biometrics cannot be used in the online (web) channel. **TPPs:** All ranges of credentials should be supported and indeed biometrics can be used in the online (web) channel if implemented in a de-coupled way that would allow the PSU to use biometrics to e.g. authorise payments at point of sale and use biometrics to authorise a payment in the online (web) channel e.g. the mobile bank-id authentication procedure in the Nordics enables.	**4**
		31. Should allow the transmission of credentials by or through AISPs and PISPs (forwarding of credentials) where applicable.	Y	Y	For credentials that are transmittable by the PSU, ASPSPs shall provide interface(s) through which PSPs can transmit the credentials issued by ASPSP to their customer. For example, these may include a static password and OTP/TAN. The API should include the option to allow the PSP to transmit PSU credentials (along with user name/identifier) to the ASPSP. Additional authentication steps between the PSU and the ASPSP in this scenario are not necessary. The process journey for authentication (web/app/mobile etc.) of the PSU should not be more complex or involve unnecessary steps.	**2**
		32. At least each of the following methods for authentication procedures should be supported by the API initiatives: (i) embedded (ii) redirect (iii) decoupled embedded (iv) decoupled redirect	Y	Not applicable to ASPSPs	A variety of different personalised security credentials exist and not all ASPSPs support all the same types of credentials. These vary per institution and per customer channel. The API initiatives need to support all authentication methods and processes used by ASPSPs. Allowing market choice by the ASPSP to be able to decide, as appropriate given the market context, to implement one or more SCA procedure(s) in a standardised way. Promoting choice while offering consistency is a core principle relevant to the API Initiatives. The choice to implement a chosen SCA procedure will also be guided by existing wide-ranging methods of the SCA and should not be constrained by the API Initiatives. Evolution in SCA techniques should also be considered where API Initiatives supporting each authentication procedure offers a degree of future proofing. Credentials which are **not transmittable** by the PSU include a biometric (for example a fingerprint used either by an ASPSP app or by a trusted third-party app (for example Mobile BankID in the Nordics). •APIs shall support authentication methods and processes that support non-transmittable credentials. The process journey for authentication (for example web/app/mobile etc.) of the PSU should be as straight forward as possible and emulate as closely as possible the steps that would be the case when the PSU authenticates to the ASPSP. •The PSP may design the user experience for any device or channel (for example PoS, wearables, voice etc.) with the exception of the authentication step. •Authentication can happen in parallel to the PSU-interaction with the PSP or when the PSP triggers the ASPSP's SCA (for example by sending the user name/identifier and/or IBAN to the ASPSP) which then sends a push message to the associated mobile device upon receipt of which the PSU opens the ASPSP's app or its trusted 3rd party app to authenticate using a biometric. •It is also important that the end-to-end process is not limited to a single device, but that the PSU can interact with the PSP e.g. at PoS while the SCA only is done at the PSU's smartphone, even if it would be possible to do both on the same device (e.g. some smartphones); in other words the payment initiation and authentication processes must be allowed to happen at two different devices. For credentials that **are transmittable** by the PSU, ASPSPs shall provide interface(s) through which PSPs can transmit the credentials issued by ASPSP to their customer. For example, these may include a static password and OTP/TAN. •The API should include the option to allow the PSP to transmit PSU credentials (along with user name/identifier) to the ASPSP. Additional authentication steps between the PSU and the ASPSP in this scenario are not necessary.	**1**

					BEUC: For consumers the key question is security and whether any third party can get access to consumers' personalised security credentials. The PSD2 states that the TPP must ensure those credentials are not accessible to parties other than the user and the issuer and that the TPP will transmit it through safe and efficient channels and cannot store credentials (in case of PIS). Nevertheless, we consider this is too risky. For BEUC, it seems that the secure option is redirection (and, where warranted, the decoupled method as a variant of redirection), in other words, where no personal credentials are shared with any TPPs. **Retailers**: API initiatives should enable any of the authentication methods (embedded, redirect, decoupled embedded, decoupled redirect and delegation), as long as cryptographic and security mechanisms provide end to end security and are implemented to ease the customer payment experience. Authorisation flows should allow TPPs to innovate the user experience and integrate innovate methods such as behavioural and physiological biometrics on customer devices. It is crucial that payers have confidence on how the authentication applies and give them the opportunity to decide the type of authentication and payment experience they prefer. Allowing customers to choose between different secured payment authentication methods is key to enabling consumer adoption of new credit transfer payment methods. **TPPs:** The main means through which bank-independent fintech's compete and innovate is through the user journey which needs to be convenient and easy-to-use. Providing an alternative to redirect is the very way bank-independent TPPs have become successful, as an example, it was only thanks to the embedded flow that TPPs could offer mobile-based payments as the TPP could then design a user interface adapted for mobile devices that worked for the customer of any ASPSP despite such ASPSPs themselves not offering a mobile-adapted user interface. As a result of a better customer journey, in many European countries bank-independent PIS based on the embedded authentication method is the most widely used. Millions of European consumers and thousands of European merchants are used to such user journeys. There is no reason or rationale for imposing on these PSUs a new and less convenient payment flow which would unnecessarily remove choice for the merchant and consumers. It is crucial that TPPs can remain in control of the user experience and offer products adapted for new channels and devices, e.g. voice-enabled payments, payments at Point-of-Sale terminals, or payments at a wrist watch which would work based on the embedded authentication method but are not compatible with the redirect method. For all the above reasons, the embedded authentication method should be supported. If the ASPSP decides to also offer a redirect flow, it should be as convenient and user-friendly as possible. This means: i) for authentication methods when the credentials are transmitted by the PSU to the ASPSP and the account to be credited is not known beforehand, one step/screen controlled by the ASPSP vis-à-vis the PSU. In more detail, the TPP through the API communicates to the ASPSP amount and beneficiary account number (alongside payment scheme and payment reference number). ASPSP then does the dynamic linking, and on one screen requests the signing/authentication from the PSU. The ASPSP then communicates the payer's different accounts and associated currencies to the TPP through the API. Following this, the PSU is redirected back to the TPP interface to select payment account from which the payment should be made. The TPP communicates the account number from which the payment should be made to the ASPSP through the API and payment is executed accordingly; (ii) for authentication method when the credentials are transmitted by the PSU to the ASPSP and the account to be credited is known beforehand, one step/screen controlled by the ASPSP vis-à-vis the PSU. In more detail, the TPP through the API communicates to the ASPSP amount, beneficiary account number and payer's account number (alongside payment scheme, payment reference number and currency). The ASPSP does the dynamic linking and on one screen requests the signing/authentication from the PSU. The PSU performs the authentication and is then redirected back to the TPP interface; (iii) for authentication when the credentials are not transmitted by the PSU to the ASPSP (decoupled, e.g. biometrics on mobile phone), and the account to be credited is not known beforehand, one step/screen controlled by the ASPSP vis-à-vis the PSU. In more detail, the TPP through the API communicates to the ASPSP the amount and beneficiary account number (alongside payment scheme and payment reference number). The ASPSP does the dynamic linking and on one screen requests the signing/authentication from the PSU. The ASPSP then communicates to the TPP through the API the payer's available accounts and associated currencies and the PSU selects the account from which the payment should be made in the TPP interface (which may or may not be at the same device where the authentication is done; it can e.g. be at point of sale or desktop while the authentication is done at a mobile phone). The TPP through the API communicates the account number to the ASPSP and payment is executed accordingly; and (iv) for authentication when the credentials are not transmitted by the PSU to the ASPSP (decoupled, e.g. biometrics on mobile phone) and the account to be credited is known beforehand, one step/screen controlled by the ASPSP vis-à-vis the PSU. In more detail, the TPP through the API communicates the amount, beneficiary account number and payer's account (alongside payment scheme, payment reference number and currency) which is to be credited based on which the ASPSP does the dynamic linking and pushes a push notice to the PSU. The PSU signs/authorises the payment (which may or may not be at the same device where the authentication is done; it can e.g. be at point of sale or desktop while the authentication is done at a mobile phone). A redirection flow when the customer not only performs the authentication step but also the step of selection of account from which to pay (and any additional step) would see the PISP being unable to provide any service or product of its own. It would render the regulation of PIS/AIS utterly moot as the TPP's role would be to merely redirect the customer to the bank domain, similar to what a merchant itself does. It would be an example of a full and complete obstruction of PIS/AIS. The difference between "decoupled embedded" and "decoupled redirect" is that decoupled embedded allows the payer to carry out the payment at a device or in an environment (e.g. PoS) which is different from the device/environment where the authentication happens (e.g. the mobile phone). As an example, the payer can authorise a payment at Point of Sale by means of putting a fingerprint on its mobile phone. In "decoupled redirect" the payer is required to carry out the whole payment flow in the same device/environment as where the authentication happens.	
		33. At least one of the following authentication procedures should be supported by the ASPSP: (i) embedded (ii) redirect (iii) decoupled	Not applicable to API Initiatives	Y	**BEUC:** For consumers the key question is security and whether any third party can get access to consumers' personalised security credentials. The PSD2 states that the TPP must ensure those credentials are not accessible to parties other than the user and the issuer and that the TPP will transmit it through safe and efficient channels. Nevertheless, we consider this is too risky. For BEUC, the only really secure solution is redirection (and, where warranted, the decoupled method as a variant of redirection), in other words, where no personal credentials are shared with any TPPs. **ECSAs:** The chosen method(s) should be implemented in such a way as not be restrictive or obstructive for AISP or PISPs. The method(s) an ASPSP need to use will depend on the authentication procedures it already offers to its own PSU. It is the ASPSPs view that this requirement can be implemented in a good way that is not restrictive or obstructive for AISP or PISPs. Further to note that "embedded decoupled" does not exist according to some API Initiatives and that "delegation of authentication" would imply outsourcing which would require an agreement.	**Applicable to ASPSP only**

		embedded (iv) decoupled redirect			**Retailers**: ASPSP shall not support only redirection SCA but as well other authentication methods, as long as cryptographic and security mechanisms are providing an end to end security and are implemented to ease the customer payment experience online and in-store. Authorisation flows should allow TPPs to innovate the user experience and integrate innovate methods such as behavioural and physiological biometrics on customer devices. It is crucial that payers have confidence on how the authentication applies and give them the opportunity to decide the type of authentication and payment experience they prefer. Allowing customers to choose between different secured payment authentication methods is key to enabling large consumer adoption of new retail credit transfer payment methods. **TPPs**: The main means through which bank-independent fintech's compete and innovate is through the user journey which needs to be convenient and easy-to-use. Providing an alternative to redirect is the very way bank-independent TPPs have become successful; as an example, it was only thanks to the embedded flow that TPPs could offer mobile-based payments as the TPP could then design a user interface adapted for mobile devices that worked for the customer of any ASPSP despite such ASPSPs themselves not offering a mobile-adapted user interface. As a result of a better customer journey, in many European countries bank-independent PIS based on the embedded authentication method is the most widely used. Millions of European consumers and thousands of European merchants are used to such user journeys. There is no reason or rationale for imposing on these PSUs a new and less convenient payment flow which would unnecessarily remove choice for the merchant and consumers. It is crucial that TPPs can remain in control of the user experience and offer products adapted for new channels and devices, e.g. voice-enabled payments, payments at Point-of-Sale terminals, or payments at a wrist watch which would work based on the embedded authentication method but are not compatible with the redirect method. For all the above reasons, the embedded authentication method should be supported. If the ASPSP decides to also offer a redirect flow, it should be as convenient and user-friendly as possible. This means: i) for authentication methods when the credentials are transmitted by the PSU to the ASPSP and the account to be credited is not known beforehand, one step/screen controlled by the ASPSP vis-à-vis the PSU. In more detail, the TPP through the API communicates to the ASPSP amount and beneficiary account number (alongside payment scheme and payment reference number). ASPSP then does the dynamic linking, and on one screen requests the signing/authentication from the PSU. The ASPSP then communicates the payer's different accounts and associated currencies to the TPP through the API. Following this, the PSU is redirected back to the TPP interface to select payment account from which the payment should be made. The TPP communicates the account number from which the payment should be made to the ASPSP through the API and payment is executed accordingly; (ii) for authentication method when the credentials are transmitted by the PSU to the ASPSP and the account to be credited is known beforehand, one step/screen controlled by the ASPSP vis-à-vis the PSU. In more detail, the TPP through the API communicates to the ASPSP amount, beneficiary account number and payer's account number (alongside payment scheme, payment reference number and currency). The ASPSP does the dynamic linking and on one screen requests the signing/authentication from the PSU. The PSU performs the authentication and is then redirected back to the TPP interface; (iii) for authentication when the credentials are not transmitted by the PSU to the ASPSP (decoupled, e.g. biometrics on mobile phone), and the account to be credited is not known beforehand, one step/screen controlled by the ASPSP vis-à-vis the PSU. In more detail, the TPP through the API communicates to the ASPSP the amount and beneficiary account number (alongside payment scheme and payment reference number). The ASPSP does the dynamic linking and on one screen requests the signing/authentication from the PSU. The ASPSP then communicates to the TPP through the API the payer's available accounts and associated currencies and the PSU selects the account from which the payment should be made in the TPP interface (which may or may not be at the same device where the authentication is done; it can e.g. be at point of sale or desktop while the authentication is done at a mobile phone). The TPP through the API communicates the account number to the ASPSP and payment is executed accordingly; and (iv) for authentication when the credentials are not transmitted by the PSU to the ASPSP (decoupled, e.g. biometrics on mobile phone) and the account to be credited is known beforehand, one step/screen controlled by the ASPSP vis-à-vis the PSU. In more detail, the TPP through the API communicates the amount, beneficiary account number and payer's account (alongside payment scheme, payment reference number and currency) which is to be credited based on which the ASPSP does the dynamic linking and pushes a push notice to the PSU. The PSU signs/authorises the payment (which may or may not be at the same device where the authentication is done; it can e.g. be at point of sale or desktop while the authentication is done at a mobile phone). A redirection flow when the customer not only performs the authentication step but also the step of selection of account from which to pay (and any additional step) would see the PISP being unable to provide any service or product of its own. It would render the regulation of PIS/AIS utterly moot as the TPP's role would be to merely redirect the customer to the bank domain, similar to what a merchant itself does. It would be an example of a full and complete obstruction of PIS/AIS. The difference between "decoupled embedded" and "decoupled redirect" is that decoupled embedded allows the payer to carry out the payment at a device or in an environment (e.g. PoS) which is different from the device/environment where the authentication happens (e.g. the mobile phone). As an example, the payer can authorise a payment at Point of Sale by means of putting a fingerprint on its mobile phone. In "decoupled redirect" the payer is required to carry out the whole payment flow in the same device/environment as where the authentication happens.	
Enabling the ASPSP to send, upon request, an immediate yes/no confirmation to the PSP (PISP and CBPII) on whether or not there are funds available	PSD2 Article 65, 1 and 3 Article 36(1)(c) RTS Opinion 22	**34**. Should enable the ASPSP to support a CBPII journey, implying confirmation of the availability of funds on the payment account of the PSU with a YES/NO answer.	Y	Y		**4**
Enabling the ASPSP to apply the same exemptions from SCA for	Articles 18(2)(c)(v) and (vi), 18(3), 30(2) and 32(3)	**35.** Should enable the ASPSP to apply the same exemptions from applying SCA when PSU uses the service of the PISP and AISP	Y	Y		**3**

transactions initiated by PISPs as when the PSU interacts directly with the ASPSP	RTS Opinion 40-47	through the API, as when the PSU interacts online directly with the ASPSP or uses a payment instrument issued by the ASPSP.				🟨
		36. Should enable the ASPSP to support a mixed AIS/PIS journey in one communication session, implying three scenarios: - one SCA to allow the AISP to access AIS-regulated information and one SCA to allow the PISP to initiate a payment;	Y	Y	**ECSAs:** Explicit PSU consent for this scenario is required. AIS does not require additional SCA after the initial authentication if within the 90-day period after the initial SCA.	🟩 **4**
		- one SCA to allow the AISP to access AIS-regulated information, and no SCA to initiate a payment in case of SCA exemption for the payment transaction;	Y	Y (subject to SCA exemptions done when PSU interacts directly with ASPSP)	**ECSAs:** Explicit PSU consent for this scenario is required.	🟨 **3**
		- One SCA to allow the PISP to initiate a payment, and immediately thereafter in the same session to allow the AISP to access AIS-regulated information (one-time view only).	Y	In the process of clarification by the EBA	**BEUC:** Disagrees with this recommended functionality. **ECSAs:** Not clear if even a one-time view is permissible without SCA and could be challenging in any case because the merging of PISP and AISP roles under one SCA. The PSU needs to have given consent for both PISP and AISP and it should be crystal clear to PSUs what they are consenting to, i.e. that they are not only initiating a payment, but that they are also opening up their payment account information to the TPP. So, at least two separate consents are required under this scenario. From another angle, this scenario could be considered discriminatory against ASPSP which needs to apply SCA twice to fulfil the regulatory requirements. 1. Log in on internet banking to see the accounts and 2. Authorise payment.	🟧 **0**
Supporting the needs to mitigate the risk of fraud, have reliable and auditable exchanges and enable providers to monitor payment transactions	Article 97(3) PSD2 Articles 3, 22 and 35 RTS Opinion 27	**37.** Should support the exchange of data between the AISP or PISP and ASPSP pertinent to fraud handling.	Y	N	Under market facing agreement - requiring careful consideration in relation to the relevant frameworks across the different Member States. **ECSAs**: Risk and fraud management are considered critical functions impacting ASPSP operational risk and therewith capital requirements. This being the case, a "blanket" type exchange of data cannot be the solution as the kind of data to be exchanged are typically also sensitive payment data in that they can be used to initiate fraud. A possible exchange would need to take place in a mutually agreed, organised way that also allows close cooperation in case of a fraud detection that needs action. Market facing agreements and arrangements would need to be put in place. PSPs that want to engage into regulated activities are expected to provide the required due diligence themselves. **Retailers:** Security by design is a principle defined by the GDPR. Fraud prevention and fraud handling is an important step that has to be performed by the payment industry actors, including merchants, customers, ASPSPs, PISPs, device manufacturers, POI vendors, … Sharing data between PSU devices, PISP and ASPSP is pertinent as it supports real time risk analysis of payment transactions. A similar approach is done by the card industry using 3DS version 2 with multiple information on the payer used to assess and mitigate the fraud risk. **TPPs**: Data elements available in the dedicated interface should include the identity of the PSU, such as a personal ID number (where applicable) or in lack of that name, address and date of birth. This is needed for the effective provision of PIS and AIS. - AIS: A typical AIS use case is for a PSU to share his transaction history with a different credit institution in order to get a proposal for e.g. better mortgage terms. If the AISP can no longer get the identity of the PSU from the ASPSP then sharing the transaction history, no longer has any value since there is no way for the AISP (or the	🟨 **3**

					credit institution looking to provide better terms) to know that the shared transaction history belongs to the PSU and not e.g. a friend of the PSU. - PIS: For ASPSPs without real-time booking it is paramount for PISPs to know the aggregated amount of initiated but not yet executed transactions per each PSU, hence a unique identifier of the PSU is needed for providing PIS and therefore, if it is available to the ASPSP, it shall be made available to the PISP. Since a fraudulent PSU might use multiple ASPSPs, the identifier of the PSU must be the same for all ASPSPs, making the social security/personal ID number and where such does not exist address and date of birth, practical identification elements. TPPs under current market facing arrangements discovered and helped authorities and banks to detect and eliminate fraud.	🟨
		38. Should enable the PISP to explicitly request an SCA or to request an SCA exemption and send corresponding supporting data to the ASPSP, e.g. suggesting the payment to be initiated is high risk and that no exemption should be applied, or that it is a low risk transaction, which could benefit from an SCA exemption.	Y	N	Under market facing agreements **Retailers**: In general APIs should provide underlying functionality for merchants and their PISPs to - suggest exemptions, including the type of exemption- such as unattended terminal transport & parking, trusted beneficiary, recurring payment, low value contactless, low value remote - or to request SCA for each transaction. Retailers/PISPs need to be capable of defining the payment context and where exemptions may apply. Most remote payments are performed after the customer has enrolled at the merchant/PISP website or through apps which allow retailer/PISP to enable the appropriate customer experience in payment methods and in the overall customer journey. Some retailers have heavily invested in fraud prevention using mitigation mechanisms and transaction risk analysis. They have the ability to assess their customer risk profile as well as the transaction risk and apply the right authentication mechanism and customer experience to the shopping journey. **TPPs:** Without accommodating for this, ASPSP would in our view have difficulties to comply with functionality number 35 (applying exemptions from SCA in a non-discriminatory fashion) since it is the TPP that knows the purpose of the payment transaction, such as a transport fare or parking fee. Whenever and wherever reliable risk systems can be used to avoid PSUs having to do SCA these should be used. Many merchants have invested into such systems and their capabilities should be exploited. And there is room for further innovations in this area, which should be leveraged. Plus, merchants have arguably the best understanding of the risk of any particular transaction. Therefore, ASPSPs should be enabled to leverage that knowledge to avoid unnecessary SCAs when possible and if so desired. ASPSPs may or may not require additional liability shifting contractual arrangements, but the API should provide the underlying functionality.	**0**

GLOSSARY:

- Authentication credentials = personalised security credentials e.g. registered fingerprint, PIN, paired/coupled smartphone, card.
- Authentication procedure = use of one-time password (OTP) versus use of fingerprint.
- Authentication method = Method for relying on the authentication procedure, e.g. redirect, decoupled redirect, embedded, decoupled embedded.