European Payment Institutions Federation aisbl

8 FEBRUARY 2016

EPIF RESPONSE TO EBA CONSULTATION ON STRONG CONSUMER AUTHENTICATION

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 250 authorised Payment Institutions (PI) and other non-bank payment providers as our members offering services in every part of Europe. EPIF thus represents roughly one third of all authorized Payment Institutions in Europe. [1] Our diverse membership includes the broad range of business models including:

- 3-party Card Network Schemes
- Acquirers
- Money Transfer Operators
- FX Payment Providers
- Mobile Payments
- Payment Processing Service Providers
- Card Issuers
- Third Party Providers
- Digital Wallets

We play a constructive role in increasing payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

INTRODUCTION

EPIF welcomes the publication of the EBA's Discussion Paper on strong authentication as part of the Regulatory Technical Standards for the revised Payment Services Directive (PSD2). We also welcome its focus on enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union.

The payments industry is in a critical period as it starts to embrace mobile devices and the introduction of biometric solutions. It has a great opportunity to close security gaps whilst also enhancing the consumer experience.

EPIF supports a risk-based approach to the setting of authentication standards, based on the value and nature of the transaction and the channel by which the payment is made. To support the growth of e-commerce and mobile payments, it is also important that the finalised Regulatory Technical Standards should be applied consistently by all players in the payments value chain and by regulators in all EU Member States.

We agree with the EBA's proposals that some types of transactions should be exempt from the authentication standards, including low-value payments, payments between trusted parties, and transfers between two accounts of the same payment user held at the same PSP. Such exemptions should be symmetrically and consistently applied to all payment methods in order to secure a level playing field.

To provide market clarity, we agree with the EBA's proposal that it should provide guidance on consumers' personalised security credentials and also with the requirement that all communication channels providing access to, or transmitting, these credentials need to be resistant to tampering and unauthorised access.

We appreciate the difficulty in finding the appropriate balance between competing demands in setting strong authentication standards, such as high security requirements versus customer convenience and accessibility. Whatever the solution, it should ensure that the risk of market fragmentation is minimised and that the consumer is able to enjoy as consistent an experience as possible, regardless of which payment channel is used to complete the transaction.

Finally, we believe this topic is highly complex with significant risk that the regulations create unintended consequences. The complexity is a function of solutions that require high technical expertise of emerging and evolving technologies, which often have no standard agreed definitions or terms, being applied across actors who play very different roles. We expect EBA is already aware of this and that responses to its Discussion Paper will simply underscore the challenge. One way to minimise the risk of unintended consequences would be to have a more in depth consultation process with a wider group of actors. This is in line with article 98 of PSD2. One procedural approach that might work is to involve stakeholders with deep knowledge of the area to suggest specific solutions. While this should not be mandated it could possibly be included as guidance notes to the RTS.

GENERAL OBSERVATIONS

A Risk Based Approach

The principle of a risk based approach is unarguable. However, the Discussion Paper refers to recital 95 demanding the adoption of technologies able to guarantee safe authentication of the user and to reduce "to the maximum extent possible" the risk of fraud. We believe it is important to recognise that a zero fraud environment is impractical; rather, we should seek to find a balance between security, usability and competitiveness. Information Security techniques have evolved so much that "the maximum extent **possible**" would require huge initial and on-going investment and also require consumers to navigate the type of security required to access highly sensitive systems. Such an approach could:

- damage the development of ecommerce business in Europe
- discriminate against users where the technology becomes expensive or too complex for people to use, especially those with disabilities
- be anti-competitive. This is because:
    - the loss lies with those not adopting the strong authentication and large firms, especially the very large multi-nationals can take that risk while small start-ups or challengers cannot. The largest multi-nationals can even negotiate the risk away to its suppliers in the payment process
    - the costs of strong authentication must not be a barrier to competition from start-ups or smaller Payment Service Providers (PSPs)

We believe the likely costs of implementation strong authentication across the European online commerce market to be significant greater than the € 794 m fraud costs quoted in the paper, once all the ecosystem costs are included.

Principles for a risk based approach include:

a) The Regulated Technical Standards must allow for low cost solutions equivalent to the cost of a plastic card. For example, if a smart phone became a necessity in order to conduct ecommerce, this would be a higher cost than today and disadvantage the consumer as well as creating a significantly higher barrier to access for the financially disadvantaged.

b) Take proper account of the customer journey. This is not just that customer attrition rises as the user experience becomes more complex e.g. the implementation of 3D Secure. It is also the risk that as the user is the weakest link and the more complex the process the more user behaviors are likely to undermine strong authentication e.g. writing down or sharing passwords.

c) TS should to the extent possible avoid imposing a requirement on PSPs to make significant immediate investments in new technical infrastructure. Transitional periods should be envisaged.

Unintended consequences

Removing Mail Order/Telephone Order and paper-based transactions from the scope of the legislation is likely to lead to significant increases in fraud in that channel There are also legitimate concerns that this exclusion may lead to innovative methods of re-flagging "online" transactions to the MOTO channel.

Definitions

The RTS needs to make it clear if each party in the payment chain is a payer or if the requirements apply to just the original payer. In some cases an intermediary pays the merchant. Clarification is needed that payer always means the consumer of the good/service who pays money to the service or good provider. Another example of this lack of clarity is in the case of payment aggregator, who makes payments on behalf of lots of consumers. Is the aggregator also aa payer under the terms of this consultation?

It might help definitions to harmonise the language about actors with ISO20022. In ISO20022 there is a concept of a payment intermediary, this will help clarify the actors. This alignment to ISO 20022 can also be seen in other industry efforts, for example the W3C Web Payments activity.

Payment Initiation Service Providers (PISPs)

Importantly RTS should be in line with Recitals 33 and 93 of PSD2 to ensure continuity in the market for amongst other things PISPs using the direct access model. As such, RTS must accommodate this model by facilitating the PISP to transmit to the ASPSP the PSU's credentials (as issued by the ASPSP) when initiating payments.

In terms of a potential new PIS business model, in which the PISP would issue its own credentials, (e.g. as implied in Q18) and then be able to initiate credit transfers from payments accounts services by the ASPSP, there are several factors to consider. Firstly, as not every payment would be subject to the ASPSP's own authentication, a risk for unauthorised payments would emerge. Secondly, the ASPSP and PISP could have a different risk assessment of any given payment. Thirdly, it is unclear how the set-up would technically work. As such, this business model would likely require the development of a new "scheme".

Insurance as a solution

The RTS should not preclude appropriate infrastructures. The use of insurance to support a particular infrastructure should be avoided. Insurance is a potential major obstacle for new entrant PISs most often because, in practice, it is not available especially for new infrastructures with no claims history.

RESPONSES

Q1. With respect to Article 97(1) (c), are there any additional examples of transactions or actions implying a risk of payment fraud or other abuses that would need to be considered for the RTS? If so, please give details and explain the risks involved.

Additional examples

- Refunds based on stored payment instruments
- Refunds directed to another payment instrument
- Chargebacks
- Cancellation of cards and other deliberate 'denial of service' such as closure of accounts, removal of continuous authority mandates, etc.
- Merchants where the payment flow is a reversal/refund or other rebate

Risks from remote channels

97(1)(c) - "carries out any action, through a remote channel, which may imply a risk of payment fraud or other abuses."

Some situations that may introduce risk and/or fraud outside the PSP's coverage:

a. If the user must pass through a proxy (office location, hotel, ISP), it can be set to break the encrypted connection and inspect the information, thereby allowing for the authentication information to be captured.
b. Users may be tricked into using an attacker's wireless network that can be setup with a proxy, which breaks the encrypted connection and allows the authentication information to be captured.
c. Malware on the Users device, which is outside the control on the payment system may capture the authentication elements.
d. Bad user actions – The user does not lock or require any authentication to use their device; The user leaves information in old emails and SMS messages that provide details into what is needed; The user does not maintain physical control of the device.
e. Attackers can setup fake sites to look like the real site; Put the real site in a frame on their site to gain credibility; Have the person click something on the attacker's site that they think is just redirecting them to the real site.
    a. These setups can allow for something to be done behind the scenes to capture authentication information.
f. DNS can be attacked to redirect users to fake sites that they believe it real and the attacker connects all their communications to the real site, but capture authentication information.

Direct Debits

It is not clear whether the strong authentication requirements of 91 (1) (b) apply to Direct Debits as these are actually "initiated" by the payee or by the payee's PSP.

Q2. Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be data? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?

Principles for possession

- Data needs to be volatile to be considered physical possession elements, for example:
    - A private key secure in a tamper responsive hardware device could be considered as data as possession element, for example a Secure Element as defined in Global Platform on a plastic card, a SIM or an embedded secure element as used in ApplePay.
    - A dynamic value that changes on a token (like an RSA token or a dynamic CVV payment card) the value of the dynamic element can be considered proof of possession.
    - A dynamic value that changes using secure software on a phone (or other device?) can be considered possession, for example google authenticator, Symantec VIP
    - A secure software solution that confirms its status and the status of the device to the 'server' in real time as it is used.
    - On a typical payment card the printed CVV2 on the cardholder signature strip is considered appropriate evidence of card possession. Note it is not stored by the merchants, ISPSP or any other actor in the payment chain.

- An EMV chip transaction with generated dynamic cryptogram sent along with the payment data is proof of possession of the card. This could be read by contact interface, the contactless interface, or from an embedded EMV card in a phone (e.g. ApplePay).

- The Magnetic Stripe data read from a card is to be considered possession of the payment card - although weaker than EMV.

- An embossed card number on a card where this number is ONLY printed on the front (not used for EMV, Contactless or Magnetic Stripe) is considered as proof of possession of the card.

- An IMEI from a phone is hard to clone and should be considered as possession of a SIM Card, where this can also store payment credentials

Examples of Possession Elements

Possession elements considered appropriate to be used in the context of strong customer authentication:

i. Simple OTP via SMS / Email
    1. If delivered to a separate device than being used to access the website. (i.e. website via PC, SMS via phone)
ii. TOTP
    1. If shared secret is stored securely - properly encrypted.
    2. Shared secret changed at some interval
    3. Ideally delivered to a separate device than being used to access the website.
iii. Hardware device plugged into phone to generate OTP
    1. Ideally used on a separate device than being used to access the website.
iv. Hard Token separate from any user device.
v. Software based - soft token on the device
    1. If used on a separate device than being used to access the website. (i.e. website via PC, soft token app on the phone)
vi. Client certificate on the device tied to the User
    1. This would be used in conjunction to strengthen other possession elements, but cannot stand as the possession element on its own.

Control over passion elements

Possession elements can only be controlled by the PSU -

i. If the user is accessing the site using the same device that will get the secondary value, it prevents an attacker from remotely gaining access to an account on a website, but does not prevent access if the physical device is compromised or stolen. This can include bad user actions, such as not locking devices and requiring a password to access the device.
ii. Solutions such as a hard token separate from any device used to access the website provide the best attempt to ensure the PSU is accessing the site, but also does not provide the ease of use customer experience and depending on the risks may have a cost that is too much.
iii. In the end, to accommodate the user requirement, where access is all via a mobile device and is quick and easy, a compromise of risk and risk acceptance must be determined.

Indicators of strength

The table below gives some examples of possession elements and an *indication* of their strengths though this will vary with, and depend on the business model in which they are applied.

Credential	Factor	Comment	Strength (note (1) weak credentials can provide strong authentication when used as part of multifactor or multi credential authentication (2) the strength depends on, and varies with, the business model in which the credential is operating)
CVV (CV2)	Possession	Because PCI restrictions forbid storage of the CVV, the knowledge of this is considered possession of the card. However is should be considered weaker than other possession types due to ease of 'skimming'	Weak
PAN	Possession	PAN and CVV might be also consider as Knowledge Factors as user don't have to physically possess card when initiating transaction. (e.g virtual cards)	Weak
EMV PIN	Knowledge		Medium
Online PIN/Password (3DSecure)	Knowledge		Medium
EMV Chip	Possession		Strong
Address (AVS)	Knowledge	Whilst AVS is usually consider knowledge, when used in	Weak (Strong if used in conjunction

		conjunction with shipping of good/services to that address, it is considerably stronger and might be considered a possession factor	with shipping and receipt check)
Fingerprint	Inherence		Strong
Cryptogram	Possession	Whilst Cryptogram is data it is derived from the possession of a token. Even if this is not stored in a hardware solution it could be considered possession if the software solutions are considered sufficiently tamperproof	Strong
IMEI	Possession	Whilst cloning of IMEI is possible, it typically involved access to the device to insert a hardware shim. Therefore is should be considered a strong possession.	Strong
Vein Print	Inherence		Strong
Iris Scan	Inherence		Strong
Magnetic Stripe	Possession	Weak due to cloning possibility	Weak
Transaction Patterns	Inherence		Medium/Strong
Typing Cadence, Writing Gait	Inherence		Strong
Voice Print	Inherence		Strong
Time Limited SMS code	Possession		Strong
Device fingerprint	Possession	Technical implementation based on the identifiers provided by software elements can be cloned.	Medium to Strong

		Technical solutions based on the fingerprint generated by the electronic circuit can be considered Strong. Refer to "PUF technology" (Physical Unclonable Functions) for further detail.	
User behaviour	Inherence	The collection of data inherent to how a given user makes use of his computer (including, browser cookies, browser identification, add-ons or plugins installed, etc) make possible to characterize the user.	Medium to Strong

3. Do you consider that in the context of "inherence" elements, behaviour-based characteristics are appropriate to be used in the context of strong customer authentication? If so, can you specify under which conditions?

Yes, we strongly believe that transactional patterns of behaviour is strong customer authentication. For example historical behaviour of a payment instrument or consumer behaviour can indicate strongly that the payment instrument is in the hands of the consumer. This can be considered a factor for authentication but behaviour based elements provide some support to aid in creating strong customer authentication, though not provide strong value on its own. Behaviour based characteristics should not be a requirement at this time, but should be permitted. If reliable solutions are developed and proven, then requirements can be added.

We would add that voice authentication is also a behavioural based characteristic and can be considered strong

The conditions include:

- Enrolment considerations would also need to be taken into account
- Inherence needs to have a target false positive vs false negative rate to be considered usable in the real world.
- Strong Customer Authentication (SCA) based on behaviour-based characteristics should be compatible with the provision of payment initiation services.

Inherence elements such as fingerprints and others can have a certain unreliability associated with them. As well as the fact that if the information is compromised, it cannot be changed.

4. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to the independence of the authentication elements used (e.g. for mobile devices)?

- Enrolment, when the mobile phone has to be in possession of the user must be extremely strong during provisioning of the Personal Security Credentials (PSC) (see further views in question 6).

- The historical commercial failure of provisioning PSC into secure elements on phones and sim cards will be a challenge to implementation.

- Chain of custody of the device, to ensure that the device is in the hands of the consumer. Controlling the device and the software on the device makes it less challenging to provide strong customer authentication. This can be addressed by controlling the software, as extensive real time checks can be performed on the device and the application. This includes the full range of expected security checks – jailbreak / rooting, malware, location, user behaviour, application check-summing (confirms the application has not been tampered with), device ID information etc.

- Accessibility - the authentication elements have to be usable to the broader population e.g. users without access to a smartphone; network dependency on IP connectivity; reliance on a single device that, if lost, contains all the information to commit fraud; ability to use the strong authentication on a device at the same time as shopping on the device etc.

- Mobile as a single device holding multiple factors can be compromised more easily than multiple devices e.g. If the handset is lost or stolen and the code unlocked, the fraudster has access to my SMS, email, banking, ApplePay, provision Biometric, password reset to iCloud. This inherently makes multiple factors vulnerable.

- Smart phones have taken over and will continue to grow. Users want everything to be available or accessible by their smart phone.

- Users are not worried about security, in general. Users are more focused on ease of use, speed, etc. and will implement any shortcut that requires them to do less. (i.e. allow browsers / apps to cache login information) Implementing great security controls can lead to perceived poor user experiences. Implementing authentication mechanisms outside the mobile device is becoming more difficult and expensive and less accepted by the user community. (Depending on the solution, target audience and size of audience) This may drive poor user behaviours that undermine the security features.

- The security features must be compatible with inexpensive mobile devices or risk pricing out lower social economic groups from the internet which often provides cheaper cost options.

- The security features must be accessible while using the mobile device on the site where the purchase/transfer is hosted

- The security features must be manageable by those with even moderate disabilities e.g. failing eye sight; arthritis etc.

5. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?

- EMV contact or contactless does not support today a signed data element which identifies the Payee (the merchant). The same applies to other current solutions for consumer to business. So the time to upgrade EMV is typically 10+ years - as all cards and terminals have to replace or upgraded. Currently the data signed from the terminal is typically a random number and the amount.

- We would like to understand business need for this with legacy global networks, as the payee is effectively protected in the payment network, and provided to the ASPSP through the payment network. The ASPSP typically provides Payee information during or after the transaction (e.g. card notification via SMS or ApplePay notifications).

- Allowance also needs to be made for the fact that systems do not run on-line 100% of the time and an ability to replay transactions is a required e.g. to reverse a systems error.

- We do not think it is practical for consumer payments at retailers, but may be for direct credit transfers.

- Example problematic scenarios for dynamic linking:

    1. Restaurant bill with variable tip
    2. Settlement where foreign exchange changes the representation (change of currency) or changes the value (due to swings in rate)
    3. Damage deposits (e.g. Hotel)

- Technology independence. It cannot be that we need a payment card (with an additional signing device) or analogue virtual to achieve a transaction based on a Bank Account.

More generally, the interpretation of dynamic linking needs to be clearer. The interpretation is that dynamic linking is the nonrepudiation related to the payment being made by the PSU in that they

authorized the action and the integrity of that action has been maintained. If the interpretation is correct, this would be two separate items.

- First the PSU identity must be validated by the authentication mechanisms used.
- Second, once in the application, the identity has been established and the actions taken by the user must be properly logged to ensure that nonrepudiation can be performed to ensure the payment details were entered/directed by the user and any changes made along the way were performed by authorized personnel, as well as, what the changes were.

Another interpretation is that a payment would be made on behalf of a PSU using their authentication credentials? Is the dynamic code for example, an SMS alert stating a payment has been authorized in the amount of $xx to <person>, so the PSU can stop it if not authorized by them?

Overall, we were unclear on the intent of what is being covered with the dynamic linking and dynamic code.

6. In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?

- ApplePay comes close - however all authentication factors are on a single device, and the PAN is re-used (non dynamic), the EMV technology does not dynamically link the transaction to the payee (see point in Q5).

- CAP tokens (as using for banking in the UK for example) are another example – however, this technology is being withdrawn due to a very poor customer experience which the EBA proposals are in danger of replicating. Solutions like these can be in software in a banking app (e.g. Barclays) which is a slightly better experience, but not a panacea. We recommend that the EBA look at the UK experience of introducing CAP tokens and the difficulties of adoption due to very poor customer experience.

- Any solution adopted need to be compatible with the provision of payment initiation services so as to avoid that ASPSPs effectively use the authentication solution as means to hinder PISPs to provide their services. As an example, the authentication cannot be fixed to a certain IP number. For instance, aggregators/payment facilitators are an important part of the PSP market and they need to be able to present the credentials on behalf of the PSU

7. Do you consider the clarifications suggested regarding the potential exemptions to strong customer authentication, to be useful?

The concept of trusted payees can be applied in the context of cards, for example behaviour can infer lower risk and reduced authentication for a specific transaction at a specific retailer.

Consider mobile, where there are 1000s of data points available to identify the device, its behaviour, its sensors etc. Similar technology exists and is in use for a PC browser. One challenge for this approach is who has the interaction with the device / browser? If this is, for example, the merchant who just sends the payment information the processor cannot collect the data to do the analysis.

8. Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical standards?

- Any exemptions should be symmetrically and consistently applied to all payment methods in order to secure a level playing field.
- Chains of trust should be considered, where the payee has authenticated the payer the liability should be on the payee. This will allow the "account on file models" to continue.
- See above on our points on the exclusion of telephone orders.
- Re. paragraph 43. We suggest that the channel used is mandated to be flagged to everyone in the ecosystem. This provides more information to enable risk based decisions about the transaction. This should be flagged at the earliest point in the transaction chain.

9. Are there any other criteria or circumstances which the EBA should consider with respect to transaction risks analysis as a complement or alternative to the criteria identified in paragraph 45?

- Re. paragraph 45. This needs to apply to payer as well as payee
- See Q8 response

10. Do you consider the clarification suggested regarding the protection of users personalised security credentials to be useful?

Yes: PSPs in the chain need to be able to identify payment users (payee and payer) to allow management of the risks in the payment chain (e.g. fraud and money laundering). This is key to enabling risk based authentication and exceptions to this.

a. The PSP can attempt to securely provide the PSU with credentials, but the PSU has to be responsible to protect the information given to them, their email, their device, etc.
b. The PSP must properly protect the authentication information stored in databases, etc. under their control.

11. What other risks with regard to the protection of users' personalised security credentials do you identify?

See Q10 response. The more anonymous the payment credential, the harder the management of risk.

a. The PSU is the greatest risk as it relates to their personalized security credentials. As stated, loss of device, phishing, scamming, social engineering, fraudulent sites, device hacking, etc. There are so many ways that from a user perspective the security credentials can be affected.
b. On the PSP side, proper encryption at rest, encryption in transit, proper application controls, logging, proper call centre procedures, etc. need to be in place to ensure the security credentials are not exposed or account access provided to the wrong user.

12. Have you identified innovative solutions for the enrolment process that the EBA should consider which guarantee the confidentiality, integrity and secure transmission (e.g. physical or electronic delivery) of the users' personalised security credentials?

End2End encryption (when done well)

Novel techniques for the identification of the cardholder using point or sale and ATM technology.

- Delegated authenticated to a trusted third party
- FIDO (Fast Identity Online) allows for a standard way of authenticating on a device.
- SCAI - stacked countersignatures attributes implementation
- Quantum information processing (an emerging field) can protect data in communications, if you observe it, the information disappears by magic. See Quantum Base, and papers by Prof Robert Stevenson (Lancaster University)

However, the above do not deal with enrolment which remains the critical challenge in any credential system

13. Can you identify alternatives to certification or evaluation by third parties of technical components or devices hosting payment solutions, to ensure that communication channels and technical components hosting, providing access to or transmitting the personalised security credential are sufficiently resistant to tampering and unauthorized access?

Implement requirements in line with other frameworks to allow for the leverage of compliance with those to aid in the verification of the controls such as PCI-DSS, Cybersecurity framework, ISO framework.

14. Can you indicate the segment of the payment chain in which risks to the confidentiality, integrity of users' personalised security credentials are most likely to occur at present and in the foreseeable future?

The largest issue is the user and the users' device. Users generally do not worry about security, but more about ease of use and speed. This leads to unlocked devices that contain applications with open access to all their information (email, bank sites, etc), unpatched devices, phishing or social engineering, malware, pop ups on certificate errors dismissed. The Payment Service User is also the biggest risk to confidentiality.

If the EBA RTS introduces a complex process for PSU and a poor PSU experience there is a real danger that this will increase the risk of leaking security credentials as PSU seek to circumvent the strong authentication processes.

15. For each of the topics identified under paragraph 63 above (a to f), do you consider the clarifications provided to be comprehensive and suitable? If not, why not?

a. Yes - use the Open Bank Working Group (OBWG) reference and W3C definitions
b. Yes - note it is not clear how the role of merchant payment processors works with this model, for example the PIS actually connects indirectly to the ASPSP via an acquirer, which does not fit into this model. Please clarify the role of merchant payment processors (aka acquirers).
c. Yes - use common web standards at the PSU end. But for the PIS, AIS and the ASPSP this would need to be a new standard based on ISO20022
d. Yes -
e. Yes -
f. Yes -

16. For each agreed clarification suggested above on which you agree, what should they contain in your view in order to achieve an appropriate balance between harmonisation, innovation while preventing too divergent practical implementations by ASPSPs of the future requirements?

In our opinion, RTS should set up the general framework within which ASPSPs, PISPs and AISPs operating on national or cross border level collectively will be able to develop open, technically neutral and interoperable standards. RTS regulations shall acknowledge that any PSP operating within the specific standard developed in line with RTS should be considered as compliant with PSD2. Implementation of standards should be possible with local conditions.

17. In your opinion, is there any standards (existing or in development) outlining aspects that could be common and open, which would be especially suitable for the purpose of ensuring secure communications as well as for the appropriate identification of PSPs taking into consideration the privacy dimension?

Again, we suggest making use of the OBWG.

The RTSs shouldn't preclude appropriate infrastructures: Although infrastructures should not be mandated by the RTSs, neither should they be precluded. Especially since the need for insurance would seem a potential major obstacle for new entrant PISs. If a scheme were introduced that reduced risk, analogous to card schemes / ATMs, then the need for insurance could be severely reduced or even eliminated. It would seem appropriate that any such infrastructures should be prepared to self-regulate against appropriate entry and rule setting criteria as in the PFMIs.

Relatedly, the need for insurance would seem a potential major obstacle for new entrant TPPs. If a scheme were introduced that reduced risk, analogous to card schemes / ATMs, then the need for insurance could be radically reduced or even eliminated.

There are serious practical concerns making all TPPs have to obtain insurance to cover the risk for ASPSPs and their customers in the event of TPP liability beyond TPP capacity to pay.

- Insurance is likely to be difficult to obtain: Insurance was suggested as a solution for client cash segregation. But in practice, this has not proved the case. As an entirely new market insurers will find it hard to understand. Especially for new innovative business models.
- Even if it could be obtained it would likely be costly: any insurance that is mandated by regulation tends to be very expensive unless steps are taken to encourage a competitive market.
- Insurance is unlikely to be sufficient to cover the risk: Even if insurance is possible to obtain, there is still scepticism if it will work in practice in the event of TPP default. The TPP will have negotiated it, probably in its home jurisdiction, with greater concern to reduce cost than to cover all risks. Claiming by multiple ASPSPs and customers from multiple jurisdictions will be a complex process.
- Therefore, making insurance a pre-condition for TPP authorisation risks severely impeding new market entrants and so limiting innovation and competition in

TPP access services.

It is suggested therefore that solutions are considered which could radically reduce or even eliminate the risk. For example, payment card schemes and ATM settlement schemes, are able to deal with similar risks using rules and processes without the regulator-imposed need for insurance. Although setting up new schemes is not easy and membership rights have to be agreed, if schemes or central services were introduced which similarly reduced the risks of TPP default, this should logically lead to reduction or elimination of the insurance obligation. It would encourage the development of such services if there were some acknowledgement of this possibility in the RTSs. Risk reduction could be achieved by adopting processes such as processes to facilitate the reimbursement of losses created by TPPs, e.g. with specific message types, agree error categories, agreed admin charges etc.

18. How would these requirement for common and open standards need to be designed and maintained to ensure that these are able to securely integrate other innovative business models than the one explicitly mentioned under article 66 and 67 (e.g. issuing of own credentials by the AIS/PIS)?

Again, we suggest making use of the OBWG.

In terms of a potential new PIS business model, in which the PISP would issue its own credentials, and then be able to initiate credit transfers from payments accounts serviced by the ASPSP, there are several factors to consider. Firstly, as not every payment would be subject to the ASPSP's own authentication, a risk for unauthorised payments would emerge. Secondly, the ASPSP and PISP could have a different risk assessment of any given payment. Thirdly, it is unclear how the set-up would technically work. As such, this business model would likely require the development of a new "scheme".

A number of "use cases" should be evaluated to determine how to properly structure the framework to create common and open standards.

In our view, the credentials used to initiate the credit transfers should always be those issued by the ASPSP to the account holder, even if they are being presented by a third-party. We cannot see how anything else would work in practice. EBA may accept this, however, the last section of Q18 could imply that EBA may have something else in mind? Q 18: "*How would these requirement for common and open standards need to be designed and maintained to ensure that these are able to securely integrate other innovative business models than the one explicitly mentioned under article 66 and 67 (e.g. issuing of own credentials by the AIS/PIS*)?" (emphasis added)

19. Do you agree that the e-IDAS regulation could be considered as a possible solution for facilitating the strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalised security credentials as well as for common and secure open standards of

communication for the purpose of identification, authentication, notification, and information? If yes, please explain how. If no, please explain why.

Most likely not - the regulations cover known limited set of entities with a set solution, whereas this standard is looking to cover unlimited solutions with unlimited customers. It would depend on how the e-IDAS regulation applies to payment products: at present, given the lack of harmonization in this area – e-ID might lead to market segmentation rather than pan-European authentication solutions. In fact, we would recommend the any customer authentication solution based on e-ID should be an option rather than a binding requirement for payment providers Nonetheless, we agree this should be looked at but in conjunction with W3C web authentication, Biometrics institute, Verifiable Claims, FIDO, OAUth2.0, SAML, OpenID Connect, GSMA mobile identify, 3DS 2.0, 3DS 1, EMVCo chip based authentication, CAP banking.

20. Do you think in particular that the use of "qualified trust services" under e-IDAS regulation could address the risks related to the confidentiality, integrity and availability of PSCs between AIS, PIS providers and ASPSPs? If yes, please identify which services and explain how. If no, please explain why.

Although Islands or Tribes of trust would benefit the payment ecosystem and accelerate the implementation of Strong Authentication, services requiring this for payments are authentication of PSUs and Payees to each other via on or more qualified trust services. This would also benefit non payment services such as the AISPSP access to account to provide aggregation services for PSUs. However, the regulations cover known limited set of entities with a set solution, whereas this standard is looking to cover unlimited solutions with unlimited customers so, again, our view is most likely not.