EBF_019489

8th February 2016

EBA Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised PSD2

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that, together, represent some 4,500 banks - large and small, wholesale and retail, local and international- employing about 2.5 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth. Website: www.ebf-fbe.eu.

The European Banking Federation and its members welcome the EBA initiative to offer market participants the opportunity to provide feedback on the future requirements for RTS on strong customer authentication and secure communication under PSD2. Our objective is to propose concrete solutions to the challenges introduced by the revised Payment Services Directive within a holistic approach of the entire payment ecosystem.

We have given consideration to the difficult trade-offs mentioned in the discussion paper and have concluded that, because security and customer authentication are complex and fast changing areas, it would not be practical for the EBA to define very detailed standards that would block innovation and may have counterproductive effects. Instead, the EBA should set out the principles and requirements necessary to create an equitable and a **secure environment** with a **clear allocation of roles, responsibilities, liabilities and technical neutrality.** We think that there needs to be a degree of standardisation applied to support and facilitate efficient and effective communication between the players. The standards to be developed based on EBA requirements should therefore be **open** and developed by cross industry/multi-stakeholder Working Groups.

***

Any type of access or interface should be possible, provided they are fully in line with the open standards defined collectively and answer key basic requirements such as openness, transparency, security and interoperability. These requirements should:

- Set clear deliverables and service levels for all parties, from the payer, the payee, any regulated third party provider and ASPSP and
- Ensure interoperability for existing and future solutions available on the market.

The way they are subsequently implemented in the market (be they hardware, software, schemes…) should be left to market participants. Some countries, such as the UK, are currently considering building data standards[1] and API (Application Programming Interface) standards[2] (that include but also extend beyond the scope of the PSD2 requirements) based on open standards developed and maintained in a transparent and collaborative fashion.

Standards in this context extend to specifications and rules addressing technical, operational, business and legal aspects. The use of open APIs allows all stakeholders to participate in the payment ecosystem in a transparent way, identify each other in a secure and unambiguous manner, communicate securely and seamlessly, whilst allowing room for flexibility and innovation.

PSD2 will bring into regulatory scope new payment initiation and account information services which can be offered to both consumers and businesses. Solutions will need to work seamlessly within national communities and on a cross-border basis. In order to address the scale and complexity this entails, to promote efficiency and to avoid market fragmentation, we think it is essential the RTS acknowledge the need for transparent and fully representative governance. At a minimum, one or several public or private multi-stakeholder bodies/authorities should be empowered to:

- Develop and maintain the open standards,
- Define and monitor the rights and responsibilities of all stakeholders.
- Manage a dispute resolution mechanism
- Manage a labelling or certification system e.g. by issuing trust marks to third party providers in order to allow consumers to properly identify regulated third party providers (see under question 20) within their own country and across borders.

Whether it is organised at national or European level, a governance structure is felt to be the only way to ensure all participants receive the consistent level of service they expect (transaction timing, quality of information, security).

DISCUSSION

4.1 Considerations prior to developing the requirements on SCA

Payment fraud has a direct and an indirect impact on society (ID theft resulting in Identity fraud). The latter should receive a renewed attention from Public authorities as consumers transfer personal data to dozens of entities at a growing pace, data which end up being stored, sold and potentially abused. Organised crime is increasingly moving into this kind of activity with the clear objective to raise illegal revenues and commit fraud on a large scale. A collective approach, in a private/public/partnership should become the key priority to all European and Domestic authority. As the EBA recognises, there is a constant balance to be found between customer experience and

[1] Rules by which data are described and recorded

[2] Specifications that inform the design, development and maintenance of the API.

fraud prevention and the methods employed by fraudsters change rapidly, especially as new attack vectors open up. It is vital that those seeking to prevent fraud are equally able to adapt their approach. The risk of the EBA being too prescriptive is that the industry will be hampered from responding and reacting to cybercrime and fraud threats in an adequate and innovative way. In addition, the requirements risk becoming quickly outdated.

At government level, the "identity chain" should regain attention from the European Commission by revamping the work of the ID theft Working Group. Fraudsters are always looking for the weakest link: as stated in the Commission Fraud Prevention Expert Group report on identity theft/fraud[3], "the quality of and trust in the legal entity documents issued by governments (passports, driving licences, national identity documents…) is disparate. Such variability in type will continue and increase with moves by some countries towards incorporating biometric data". ASPSPs have to rely on the quality of ID documents when enrolling new customers and issue them authentication tools (security credentials, payment cards with PIN numbers, tokens…). As a consequence, the delivery of state of the art ID documents should be the European and Domestic Authorities' key priority if the objective is to protect the integrity of identity and the effectiveness of fraud preventative measures adopted by the payment industry.

At the level of banks, ASPSPs have been investing in fraud detection and prevention tools to remain ahead of criminals, from payment cards to direct debits or credit transfers for more than 3 decades. The pivotal importance of trust and security in payments should be considered when any new product or service is introduced into the market. In this respect, the greater the number of parties involved in a payment transaction, the bigger the opportunity risk of social engineering and phishing attacks, unless appropriate processes are in place.

Questions

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

It is rather difficult to establish an exhaustive list of potential examples of transactions or actions implying a risk of fraud as security threats are in permanent evolution.

A single authentication mechanism would not be adaptable to all present and future means of payment, from transfers to direct debits, conventional payment card or cards issued by a PIISP (based on an initial request to check the availability of funds followed by a direct debit). We would therefore recommend a principle based, layered approach aimed at protecting PSUs and payment actors from direct and indirect payment fraud (see above).

In addition to the cases listed in the Discussion Paper, the initial electronic mandate for a SEPA Direct Debit and the authorisation of the first recurrent SCT may also be subject to the same level of protection as a "normal" payment transaction.

[3] See report on Identity Theft/Fraud Prevention Expert Group. Add link

Any interaction that implies the modification of contact details, authorization mechanisms or any element necessary for the initiation of transactions exempted from the obligation to proceed to strong customer authentication or even any change to white lists must require strong customer authentication.

Payment card transactions further to mail orders or telephone orders should not be discarded as they use the same processes as other e-commerce transactions. It is worth mentioning that both mail orders and telephone orders are using less secure channels than the usual processes.

2. 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? Is so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?

Possession elements are clearly described in the EBA guidelines on the security of internet payments in the definition of strong customer authentication (EBA/GL/2014/12, Title I – scope and definitions, item 12). Whether the possession element must have a physical form or may be data or both has to be decided by the ASPSP based on its own risk assessment.

National eID cards, payment cards and mobile devices could be qualified as “possession elements”. Typical examples of data could be software tokens, which are physically secured or data securely combined with a physical element.
Whereas data stored in hardened apps or keys/certificates stored in “hardened browsers” are considered as examples of physical form.
In all circumstances, the possession element must be secure, unique to a customer and controlled by him/her. In case a PSU loses that control, an immediate revocation of his/her security credentials is critical.

Consumers now expect to perform all aspects of authentication on a single device, i.e. mobile phone or tablet. Accordingly, it would not be appropriate for the EBA RTS principles to require separate hardware tokens. Non-physical software/data tokens are more forward looking options.

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?

With regard to “inherence” elements, biometrics represents an interesting tool as it can be very appropriate to certify the identity of a person, when handled in an extremely secure environment. However, one should not underestimate the dramatic consequences in case of a compromise (reversibility problems), the ability of the customer to challenge a “false-positive” and the resistance on privacy and civil liberty grounds.

Behaviour-based characteristics cannot currently be integrated in the strong customer authentication process as they only represent an additional tool. As a matter of fact, they are only effective when used in conjunction with other elements in a holistic approach. ASPSPs can therefore decide to use them, depending on its own risk assessment as well as on the maturity of the solution and the reliability of the behaviour data. As a matter of fact, they are only effective when used in conjunction with other elements in a global approach and can be considered a useful monitoring tool but not a part of the strong authentication process. In this respect, the intermediation of PISPs, PIISPs and AISPs will result in the loss of very valuable information. Third Party Providers must, therefore, be encouraged to share any data they obtain from their sessions with PSUs with ASPSPs in order to avoid fragmentation of intelligence between several payment actors.

4. Which challenges to 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)?

As mentioned under point 18 of the Discussion Paper, customer convenience is a major topic which has to be integrated in any payment solution provided to customers. For example, customers expect that it is possible to order and pay using the same device.

Independence of the authentication elements needs not necessarily to be achieved by physically separated devices. Logical channel separation can be used to achieve the necessary independence of the authentication elements. The operating systems used by the PSU in his/her various devices (computer, mobile..), and under his or her control, must ensure proper independence of channels to protect the communication of authentication elements by the ASPSP. Because consumers increasingly expect to use one single device (tablet or smart phone for surfing and paying), manufacturers could be encouraged to enhance the reliability of their devices to the benefit of the entire ecosystem through the separation of the different elements used in the same device for the purpose of access, authentication and authorisation of a payment service.

The ASPSP has to decide, based on its own risk assessment, which solutions it implements to ensure the authentication elements are provided independently.

In all circumstances, the PSU’s devices need to be registered with the ASPSP to make sure they can be properly used to make payments or receive aggregated accounts information from AISPs.

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

The concept of “dynamic linking” should be clarified by the EBA in its requirements, with some general criteria on dynamic codes and taking into consideration the variety and specificities of the means of payment available on the market (cards, transfers, direct debits). One single solution would not be the appropriate route and risks being outdated short after its introduction.
The “dynamic link” must be comprehensible to the PSU, so that he/she is able to identify/confirm the transaction data linked to the calculated dynamic code and enjoy a seamless payment

experience. The main challenge comes from the experience proving that a "one size fits all" approach is not appropriate as transactions take place in a large variety of environments and payment patterns. The EBA requirements should be made fit for purpose in order to allow the ASPSP to adapt them to its risk analysis and the payment product issued. A risk-based approach, in addition to a product based approach, should be preferred in order to balance security requirements, user experience and PSPs' investments.

A specific attention should be devoted to the different categories of customers (i.e. corporates versus retail), whose needs and payment methods differ substantially.

Some product propositions do not encapsulate dynamic linking (recurrent transactions and 3D Secure) whilst operating in a very secure environment. We would therefore advocate for a more proportionate approach, allowing ASPSPs to decide in which environment and for which amount dynamic linking should be mandatory (high risk transactions for example).

Finally, when the transaction amount is unknown, we would recommend a zero default.

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

There may be solutions based on logical separation of the password entry and the generation of the transaction code by different apps on the same mobile device which will fulfil both the objective of independence and dynamic linking (secure storage of authentication elements in some mobile devices, touch IDs and the functionality of some SIM cards could help achieve these objectives.

4.2 The exemptions to the application of SCA

Questions

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

The categories quoted under point 42 provide useful examples to ASPSPs that decide to introduce or not exemptions to strong customer authentication in their processing system. However, the exceptions have to be optional and very dynamic so as to countermeasure the industrialization of cybercrime.

Being responsible for securing its clients' assets, it is indeed up to each ASPSP to individually define its security policy and what type of transactions should require strong customer authentication, based on its internal risk assessment. An ASPSP or a group of ASPSPs can, for example, decide not to manage white lists or require strong customer authentication for purely consultative services. Equally, it is up to the ASPSP to define the transaction limits on contactless payments. Such decisions should remain at its discretion.

An exhaustive list of possible exemptions cases may not be future proof and even counter-productive and not allow future innovations based on new criteria unknown today which may be adopted in a few years down the road. We therefore agree with EBA approach to consider that the five transactions categories listed under 42 as mere examples.

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

A principle risk based approach is paramount when deciding about exemptions. In this respect, the list provided in the forthcoming regulatory technical standards should not be exhaustive and should remain principle-based.

It is up to each ASPSP to assess the risk for each transaction, be it recurrent or not. Dynamic linking would, for example, be systematically required for ad-hoc high value transactions, in addition to other authentication parameters (behaviour based…). One could also think of authentication solutions based on a physical element (a payment card, a smartphone,..) and a security mechanism integrated in this element that allows the use or generates a unique password.

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

As said above, a risk-based approach is the most appropriate to allow PSPs to take into account a multiplicity of factors, adapt their risk policy to a fast changing environment and react rapidly to any change of circumstances.

Taking a broader view, data sharing for fraud and cybercrime prevention purposes across the payment industry should be encouraged and allowed by the Regulatory environment and extend to essential external partners such as the police and intelligence services. It is indeed only when all the pieces of the puzzle are pulled together that actors can react quickly, adopt preventative action and identify criminal gangs. Availability of these data can support the transaction risk analysis in a very efficient way, providing ASPSPs with very valuable information to prevent and combat fraud, cybercrime and, ultimately, fight against terrorism.

Computer Emergency Response Teams (CERT) offer the appropriate framework to prevent fraud and ensure cooperation among all stakeholders. Unfortunately, there is no appropriate structure at European level to ensure a Europe-wide management and prevention of fraud and cybercrime. We would therefore encourage EBA to issue standardized pan-European requirements to allow for an efficient sharing of intelligence (sensitive and personal data) on an EU-wide basis.

4.3 Protection of PSU security credentials

Third Party Providers do not need to have access to such sensitive data to keep offering their services. To a PIISP (card-based payment instrument issuer) or a PISP, information on the availability of funds or proper authentication of the payment is sufficient. AISP do not need to have access to the whole payment account but only to the information the PSU deems important to aggregate his or her account information.

Most existing communication platforms (Facebook, Google or Amazon or an API for example) do not require the storage of credentials or to make them accessible to third parties as they generate access tokens that will allow free and secure access. In these environments, customers remain in full control of the type of data they make available to third parties. Making master credentials available to a third party does not allow consumers to have a detailed understanding of what information they share and for how long. Encryption end to end needs to be looked at as a safe method as it removes the risk and hence the liability from the TPP, allowing a wider access to new entrants. Providing encrypted tokens does not affect the current customers' experience as they can continue to transact in a safe and easy manner whilst keeping their credentials safe, in line with PSD2 (article 69.2).

<u>Questions</u>

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

The clarification suggested is useful. However, credentials/passwords should never be stored. Security standards and protocols such as OAuth or SAML can be used, without the need to store credentials.

As said above, users' personalised security credentials (hereafter referred to as "PSCs") can only be protected if they are not shared or made accessible to third parties. This is the reason why PSD2 clearly recognises that customer credentials are "sensitive payment data which can be used to carry out fraud" (see Article 4.32). The consequences would even be dramatic in the Nordic countries as is would result in an effective handing over of credentials for eID and electronic signatures for general purpose certificates (within the eIDAS Regulation). Making these credentials accessible to third parties would have devastating effects on the society as a whole.

Besides, access by TPPs to these credentials contradicts the very objective of PSD2 to increase the general security level for all payment actors and represents the greater risk even though the objective of PSD2 is to increase the overall security level for all payment instruments and all stakeholders. Therefore, it makes sense to ensure that the sole control of the PSC is rested with the user and the ASPSP that has issued them.

An API enables a customer-driven ecosystem. The customer is in control of what can and cannot be shared with a third party, as the API is consent driven. Making credentials accessible means that the third party has the ability to access and edit any information the customer is able to see and change; this removes the ability for customers to have full control over what information is shared and for how long.

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

It is of paramount importance to avoid any technical solution that implies the access to PSU's PSCs by TPPs or any other third party. Therefore, the PISP and AISP access to user's PSCs must be clarified with regard to Article 66 and 67 of PSD2, as PSCs can only be known to the PSU and registered at the ASPSP. The intermediation of third parties into the payment chain increases the risk situation for the affected PSPs, the financial sector and the public at large. ASPSPs must redefine their own fraud management processes, should they not be in a position to control the whole payment chain anymore. If there would be a possibility for TPPs to obtain PSCs of PSUs, fraudulent parties could simulate to be a PISP/AISP/PIISP and use the "man-in-the-middle attack" to misuse them and perpetrate fraud.

Compromise of third parties' systems and processes, fraudulent third party providers and insider attacks of third parties cannot be excluded. Besides the risk of social engineering, risks may also result from fake certificates, outdated information in the relevant registers, centralised infrastructure, apps and data security measures implemented by payees. The same credentials will probably be used in several services having linkage to payment/bank accounts. Users do not always know whether a means of payment provided in online shopping is actually safe. We would therefore advocate a wide adoption of publicly issued trust marks to allow consumers to be assured they are contracting with a secure payment provider (see under question 20).

In more general terms, the communication protocol between PISP/AISP/PIISP and ASPSPs must ensure that transactions and payment data are protected from attack vectors. For example, an API may be providing the appropriate platform to organise secure and seamless communications between all stakeholders in the payment ecosystem.

At PSU level, personal devices are most certainly the less secure environment for making payments or consulting payment accounts, despite all public and privately led information campaigns aimed at encouraging the public to secure personal devices

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?

All processes related to the issuance and integrity of PSCs should be controlled by ASPSPs end-to-end using secure processes. In this respect, the forthcoming EBA requirements should provide that PSC are transmitted directly between the ASPSP and the PSU, the tokens resulting from the authentication process can subsequently be shared between the AISP/PIISP/PISP and the ASPSP.

In a payment card environment, enhanced mobile solutions are being deployed to secure the enrolment, confidentiality and integrity of the PSCs either in the hardware of the software of the mobile.

13. Can you identify alternative 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 credentials are sufficiently resistant to tampering and unauthorized access?

As said above, making bank credentials available to third parties does not represent the state of the art solution to make payments. A forward looking approach should allow third parties to benefit from all the services and information they need without any need to share such sensitive data.

Different approaches are possible, provided that the necessary requirements/standards/protocols are met. The ASPSP has to decide which third parties are accepted for evaluation and certification, such as internal experts of the ASPSP, banking associations, schemes, EMVCo, PCI,…

It is worth recalling that ASPSPs are already subject to numerous certification and auditing processes; in these circumstances, it would be desirable to avoid redundancies and inefficiencies and focus on a coherent approach of the interfaces between all stakeholders.

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 device of the PSU remains one of the weakest segments in the payment chain, together with any intermediation between PSUs and their ASPSP, from the mobile smart phone to third parties. Each node adds an extra risk. One should therefore not focus on one particular segment as threats will always move to the next weak point and evolve.

Consumers' education is key and any message leading them to think they can share their credentials in one way or another would ruin decades of communication from industry and authorities. PSPs have promoted extensive information campaigns over the last decades to educate their clients not to share their credentials with any third party, be it the PIN code of their cards to their home banks' security credentials. Making them believe that they can make their credentials available to some third parties would break a psychological barrier that will put the entire security infrastructure at risk. The EBA should also consider the customer education necessary for a proper use of these new payment services.

Second, one cannot expect consumers to be in a position to distinguish a trustworthy TPP from a fake TPP.

Any future standard must allow payment providers to be one step ahead of criminals and help the payment ecosystem to move forward in a secure manner. Alternatives should be sought to provide third parties with all the information they need to process their clients' request in a secure and competitive environment.

4.4 Secure communication

Questions

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?

In addition to AIS and PIS providers, PIIS providers should also be considered as a third category of TPPs. Card-based payment instrument issuers offer a very specific product to payees that is quite different from the services provided by PISPs. We understand that ASPSPs will need to provide a confirmation on the availability of funds to PIIS providers at the time of the request based on a card that will have been presumably issued to a PSU. It is rather unclear at this point in time whether and how the PSU's consent will have to be made known to the ASPSP. Equally, the way card transactions are subsequently processed should be analysed in detail as they differ substantially from conventional payment cards that generate a single payment transaction (that is authorised and guaranteed by the card issuer), not an initial request followed by a payment transaction. We indeed understand from PSD2 (recital 68) that this type of service requires two different types of messages, the first aimed at confirming the availability of funds at the time of the request (without blocking the funds – see Article 65.4), followed by a direct debit. A detailed analysis of the entire process should be undertaken to assess the challenges of this type of product (i.e. the security level of the card issued to the PSU), risks and respective liabilities of all parties involved and it deserves a specific approach when designing the forthcoming requirements.

As a general comment, and in order to ensure competition and interoperability, the standards must be usable by any participating provider and must be free of any rights of any other parties and be based, whenever possible, on existing standards.

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?

As stated in our introductory statement, a clear governance of standards, communication channels between all stakeholders is indispensable to securing aggregation and payments on the internet, independently of the identity of the provider (AIS, PISP, PIISP and ASPSP).

The clarification and requirements of the RTS must incorporate at least the following issues:

a) All types of means of payment should be treated separately as their processes are not identical (payment cards, transfers, direct debits)

b) "Open and common standards"
Any interface set up in the EU must be exclusively based on open standards, agreed upon by all stakeholders involved, and must be applied in a consistent way for any third-party services and application scenarios.

c) “PSP Identification

A formal process must be established, with a neutral entity, for registering, licensing third-party services and certifying PSPs by issuing watermarks that guarantee the identity of the PSP to the public at large (see under question 20).

This process must be transparent for all parties involved, setting out clearly-defined criteria as to which requirements must be fulfilled for registration or licensing. All registered and licensed third-party services must be listed in a central, uniform register that applies throughout Europe. This European central register should be legally binding in the same way as the various registers kept at National level by the competent authorities.

d) “Secure communication”

The authentication of the AISP/PISP/PIISP towards ASPSPs has to be secure i.e. using certificates (see under f). The communication interfaces between PIS/AIS-provider and ASPSP must be accessible by all participants regardless which mechanisms have been used for the authentication of the PSU.

e) “Minimal functional requirements”

Using parametrization should make the interfaces flexible and open for new scenarios. The interfaces must be designed in a manner that allows for version handling at a protocol level: Communications using different versions must be supported on the basis of clearly-defined version information within the protocol.

f) “Security controls”

The authentication of the PSU by AIS/PIS-provider should be based on the authentication provided by the ASPSP using PSC issued by the ASPSP.

g) “Technical requirements”

The interfaces should be based on commonly-used internet-standards (such as XML, XML Schema, XML Signature, Web Services, JSON or REST-API). The interfaces protocols must provide for transparent error handling and flow control for big size messages.

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?

As already stated under question 16, the interfaces should be based on commonly used internet standards. Electronic seals could be used for the identification and authentication of AIS/PIS/PIIS – provider and ASPSP. Please note that electronic seals (as defined under the eIDAS Regulation) cannot be used for payment authorisation – see below under question 19.

OAuth/SAML, an open authorization standard commonly used at international level suits those purposes. EBA should avoid developing standards only applicable at European level as it would introduce unnecessary barriers for European payment actors.

18. How would these requirements 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) ?

The requirements to be set by EBA should: not allow for a different approach for ASPSP-PSU interaction than for the AISP/PISP/PIISP – driven interaction.
In more detail:

- The specific security and/or authentication must be transparent for the interfaces, i.e. the interfaces format specification should not force the user to apply certain types of authentication.
- Security procedures must be described in a sufficiently high level manner in order to be technologically neutral.
- The procedures must be referenced through unique identifiers (or profiles).
- The communication partners (AISP/PISP/ASPSP) have to use these identifiers to uniquely identify the security procedures (padding, hash procedure, type of signature) and processes for both partners.
- Interface specification must be sufficiently strict in order to prevent ambiguity or individual interpretation, whilst maintaining the necessary flexibility as the same time.
- Technical parameters and protocols must be sufficiently harmonised to allow any third party provider (AIS/PIS/PIIS-provider) to establish a connection to an ASPSP.
- The interfaces must be designed in a manner that allows the handling of different versions.
- Access to all standardized and approved versions must be supported.

4.5. Possible synergies with the regulation on electronic identification and trust services for electronic transaction in the internal market (e-IDAS)

Questions

19. Do you agreed 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.

Whereas it is uncertain that the eID can be easily rolled out in the private sector, it should be limited to identifying customers and not be extended to authentication.

A clear distinction must indeed be made between the identification of the individual (that can clearly rely on eID issued by public authorities), strong customer authentication (algorithm provided by ASPSP) protection of the confidentiality and integrity of the PSC (under the responsibility of the ASPSP) and the secure communication between participating service providers.

Strong customer authentication: The electronic identification mechanisms/schemes regulated by e-IDAS cannot be rapidly adapted to the realization of strong customer authentication within payment services or account information services in all European countries. Some countries have a more mature adoption of the eID that has been deployed outside of public services. However, a complete roll out of eID in the private sector on a pan-European basis is not a realistic perspective in the short term.

Protection of the confidentiality and integrity of the PSC:
The e-IDAS regulation does not (to the best of our knowledge) contain any solution for the protection of the confidentiality of the PSCs of a PSU. Only high level requirements exist, but these do not give more details than the corresponding requirements of the PSD2.

Secure communication between participating service providers (AIS/PIS/ASPSP):
In order to establish a secure communication between an AIS/PIS-provider and an ASPSP, the communication partner have to be authenticated securely by each other. As part of this authentication it has to be proven that the AIS/PIS-provider has been registered/approved by EBA and that this registration/approval is still valid. In addition, it has to be proven the status of the provider, i.e. whether it is an AIS-provider or a PIS-provider (since the services an ASPSP has to provide to a provider depends on its status). This authentication between the participating providers should be based on electronic seals based on qualified certificates provided by a qualified trust service provider in line with the e-IDAS regulation (see under question 20).

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.

Qualified trusted services are likely to have positive benefits: they can ensure that transactions take place in a secure environment without sharing sensitive data and help identifying payment providers. For example, in an API approach, digital certificates would be needed to secure the information on participants. It could equally solve the issue created by the non-legally binding nature of the EBA register. Nevertheless, these services should be specifically and properly be contextualised to the payment sector.

Risks related to the confidentiality, integrity and availability of PSCs

An appropriate environment can ensure AISP/PIISP/PISP are able to offer their services on equal footing with ASPSPs without having access to very sensitive data such as PSCs. Security credentials should only be transmitted between the PSU and the issuer of the credentials (i.e., the ASPSP). Tokens resulting from the authentication process between the PSU and the ASPSPs can then be made available to third parties without running any risk of being compromised.

Secure communication between participating service provider (AISP/PISP/PIISP/ASPSP):

The authentication of PIS/AIS-Provider and ASPSP should be based on electronic seals based on qualified certificates issued by qualified trust service providers under e-IDAS regulation. For this, EBA should define a policy to be implemented by the qualified trust service provider. Real-time digital interaction with digital certificate are needed to secure the information on participants as a means of ensuring that they are authorized to have the access they are requesting.

Once ASPSPs and AIS/PIS/PIIS providers can interact in a secure way, the public at large must be able to identify the third party providers that meet all the EBA requirements and are properly supervised. To that end, we would propose that a qualified trust service provider, who could be the European Commission, grants **recognizable trust marks/labels** to inform the public and allow them to interact with proper third party providers.

Compliance with this policy should assure at least that:

(a) only PIS/AIS-provider registered/approved by the competent authority or authorities will get a certificate and the corresponding trust mark/stamp (to be developed)

(b) a parameter contained within the certificate states the role of the certificate owner (i.e. AIS-provider or PIS-provider or ASPSP),

(c) if the registration/approval of a PIS/AIS-provider is withdrawn by the competent authority or authorities, the certificate must be immediately cancelled and the watermark deleted from the payment provider website.

We should mention in this respect that a real-time, on-line fully accessible and legal binding EBA register of AISP/PIISP/PISP is needed to ensure that ASPSPs (and users) can always check the trustworthiness of the payment intermediary. A purely informative register, as is planned today, would force ASPSPs and PSUs to rely on registers held at National level, introducing a substantial burden on all and administrative fragmentation in SEPA, a borderless environment by definition.

For all other services the use of qualified trust services under the e-IDAS regulation should be optional and therefore not regulated by the RTS to be prepared by EBA.