EPC020-16
v 1.0
Date issued: 8 February 2016
EPC

[X] Public – [ ] Internal Use – [ ] Confidential – [ ] Strictest Confidence

Distribution: The European Banking Authority (EBA)

The EPC Response to the EBA Discussion Paper on Strong Customer Authentication and Secure Communication

The European Payments Council (EPC) welcomes the EBA Discussion Paper and the opportunity offered to provide feedback on the future draft Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Secure Communication under PSD2.

The EPC's objective is to provide input concerning principles to be covered by the RTS that should address the challenges introduced by PSD2. The aim is to ensure a level playing field with corresponding responsibilities and liabilities for all stakeholders in the payment value chain.

General comments
In general terms, the EBA RTS should be as much as possible principle-based and not define specific technical standards or include an exhaustive list of examples. This is to allow for robust, technology-neutral, solution independent RTS, which provide for sufficient flexibility to allow evolving market solutions and innovation. In addition, the RTS must be open for all business, technical, legal and operational models and must facilitate the creation of an environment that is fair with clear delineation of risk and liability. Given the proliferation of scenarios where Payment Service Users (PSUs) need to grant authorisation to third parties (TPPs) in order to access their information, or to act on their behalf, it is fundamental that the RTS developed by EBA do not impose restrictions on the ability of (European) PSPs to develop homogeneous services at global level. In that respect, referring to the last sentence in 62 (solutions implemented by ASPSPs [should not be] so divergent that these become a barrier for AIS and PIS to provide payment account access services), the EPC would like to stress that the reverse is also true – Account Servicing Payment Service Providers (ASPSPs) should not be confronted with too much divergence in implementations by Account Information Service (AIS) and Payment Initiation Service (PIS) providers. Notwithstanding the above, and specifically in cases where interoperability between the TPP and the ASPSP is required, it is expected that clear rule-based standards or sets of specifications would be defined, to allow for an efficient implementation and communication that is also economically

feasible between TPPs and ASPSPs.

Moreover the principles for the Strong Customer Authentication (SCA) and the interoperability specifications should be based on internationally recognised and open standards.

According to the PSD2 certain credentials can be made accessible to TPPs. However, it is understood that the PSD2 aims to give PSUs control over the information that is shared this way. The RTS should take into account that when using an application programming interface (API) approach, there exist technological solutions whereby credentials are only used between the ASPSP and the PSU and yet the TPP gets the functionality and information they need. To achieve the aims set out by the European Commission it is believed that it is not necessary for PSUs to share their personalised security credentials with a TPP.

Finally as long as strong customer authentication is not imposed globally it will not result in a significant reduction of international fraud, more in particular in relation to card based transactions. Attackers will continue to harvest card data, independently of the sophistication of the strong authentication, and make use of it at non-European merchants.

Next to the RTS, appropriate governance structures may need to be set up to manage the changes that would result from a fast evolution of available technologies, risks and the payment ecosystem. Such governance structures could address the following:

- Maintain the principles and interoperability standards.
- Monitor the rights and liabilities of all stakeholders.
- Manage a dispute resolution mechanism.

Regulated PSPs, including AIS and PIS providers will have to comply with all the security measures deriving from the PSD2 (Title IV) and delegated acts (Title V). As explained in the background section of the Discussion Paper, it is important to underline that only 18 months after their adoption by the European Commission, PSPs will have to comply with the RTS on SCA and secure communication.

Given that ASPSPs and TPPs do not need a bilateral agreement to operate, ASPSPs need a mechanism to validate in a real-time automated, secure and reliable manner if a PISP or an AISP acting on behalf of their PSUs are in fact registered and, if applicable, authorised for this request by competent authorities of the home Member State. Additionally, PSUs should be made aware of the EBA register and be educated to avoid the unintentional provision of their personalised security credentials to fraudulent counterparties. (cfr 57)

1. Considerations prior to developing the requirements on strong customer authentication (section 4.1)

General comments
Irrespective of any necessary trade-offs, the RTS should ensure consistency with regard to a minimum PSC (Personal Security Credentials) level of assurance to be defined for PSD2. Common practice evidenced the fact that the PSC level of assurance provided by two authentication elements (as minimally required for strong authentication) can largely vary: from very low, for two static elements fully exposed at every authentication, to very high, for hardware-sealed static elements only used for the secure generation of short-lived one-time codes exposed for a single authentication. The PSC level of assurance thereby determines the extent to which the two authentication elements, i.e. the PSC agreed between the PSU and the PSP, may be exposed during provisioning, usage and normal safe-keeping and the extent to which they remain under sole control of the PSU (cfr. NIST.SP.800-63-2 for an example on how to possibly deal with this topic). The following paragraph aims to illustrate how the various authentication elements relate to the PSU: • With regard to inherence elements (biometric characteristics), the level of assurance relates to the level of sole control over the biometrics, which itself relates to the effectiveness in reliably verifying freshness and liveliness of static biometric characteristics during authentication. • With regard to possession elements (SMS codes to a mobile phone with a SIM card registered to a specific personal mobile number), the level of assurance relates to the level of sole control over the SMS message content sent to this number, which itself relates to the effectiveness in reliably excluding SIM swapping, second SIM, replacement SIM, SMS interception and SMS forwarding during code provisioning. • With regard to knowledge elements (static passwords or PINs), the level of assurance relates to the level of sole control over the static password or PIN, which itself relates to the effectiveness in reliably excluding password or PIN exposure to network-exposed environment, e.g. by using them only to locally activate tokens. It is expected that all requirements concerning the SCA of the PSU must hold for all PSPs to ensure a level playing field for all market participants.

Questions

1. 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.

Response:	Strong authentication should also be required whenever a given action is performed with respect to the management of the payment instrument (e.g. resetting a password, PIN, parameter update, updates of white lists, change of notification channel, etc.) upon which the process of submitting payment transactions is dependent. If the change of any given setting in this context causes to: • Alter the perception of the PSU on the true nature of a given transaction under execution (such as the amount, destination account, beneficiary name, etc.); • Facilitate the execution of recurrent or subsequent transactions which may be out of the scope of attention of the PSU; • Federate identities in the context of authentication for payments; • Change parameters that may increase the overall risk or level of impact of fraud attempts (such as the setting of transaction limits and so on); it constitutes an increased security risk and should therefore be considered in this context. Relevant issues may also arise if for example physical/email/logical addresses as well as other personal information used for relevant communication purposes for financial services are changeable via remote channels or in the subscription of new financial products/services, particularly in the case where patrimony changes may occur. In addition, the RTS should differentiate between risk increasing and risk reducing actions, where applicable, since the latter ones would typically reduce a prior accepted risk level and might therefore not require an SCA (e.g. lowering a risk parameter limit would reduce the risk).
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? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?	
Response:	Possession elements can have a physical form or can be data. Since data as possession element is more vulnerable, it would be advisable that at least one or part of the possession elements has - or is linked to – a physical form (e.g., smart cards, mobile devices,…) in the possession and sole control of the PSU. The latter depends on the security measures implemented. Examples of hardware possession elements include:

	• Specialised tamper-resistant crypto devices, which (a) Protect the possession element from being exported respectively extracted. (b) Protect the usage of the possession element by conscious approval of the user. • Disconnected crypto hardware tokens (e.g. Crypto smartcards in offline card readers; self-contained authentication tokens) • Shielded crypto hardware tokens (e.g. USB or Bluetooth dongles) with a proper level of sole control through an own trusted display and an own approval button. • Integrated crypto hardware tokens (e.g. TPMs - Trusted Platform Models) with a proper level of sole control through a trusted hardware integration of the OS. In the case of software elements, it is important adopting concrete measures regarding the software installation, the user impossibility to modify the software and other restrictions related to the devices where the software is installed. Furthermore the RTS should consider the storage of multiple sets of PSC-data (owned by one or more PSUs) within one physical device (e.g. tablet or smartphone), provided that access to a specific set of PSC-data is limited to the specific PSU that is associated with it, and that the security features of the device (access method, hardware, OS) are sufficiently reliable and secure to prevent abuse. Non-physical possession elements can provide additional PSU identification features that, used in conjunction with other independent authentication factors may lead to an increased level of certainty as to the true identity of a user who is trying to access or perform actions on a given payment instrument. The use of one or several of these data parameters under controlled circumstances may constitute a true "fingerprint" of a user and their device(s). In that sense, non-physical elements, such as pre-saved hardware manufacturers' data, installed software providers, software/hardware versions, mobile IMEI (International Mobile Station Equipment Identity) numbers, Internet Service Providers, IP addresses, or, more conventionally, digital certificates should be allowed to play a role in this context. The issue of PSU control is of course a relevant one, although, per se, no logical or even physical possession element can be considered to be 100% safe against the variety of attack vectors found in the payment industry context nowadays. Adequate risk control settings should be enforced for the various types of identification elements and will no doubt change according to the nature of each element. When elements such as hardware/software manufacturers are used, such "fingerprint" data should be gathered in "conventional" strong authentication circumstances, so that these settings are saved for reuse in a trusted environment.

	On the other hand, when mobile features are involved and particularly when mobile payment instruments are used it seems relevant to ensure that no "jailbreak" / "root" procedure has taken place on the used device, as such manipulation of factory settings could render the device more prone to the installation of malware and the compromise of security features. Naturally, such features can only be used for proper user identification if online monitoring, registering and analysis is made of them, so that the payment instrument is able to perceive changes dynamically and raise authentication standards in real-time, when deviations from registered standards are encountered. In any case, the use of physical and non-physical/logical elements has to be made under a clear awareness of the PSU, within a setting that clearly states the risks involved and the need for adequate protection practices that also involve the PSU's knowledge/actions. Raising such awareness is a key factor to ensure that PSU adoption and use of these elements is made in a way that risk concerns are tracked and reduced.
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?	
Response:	Behaviour based characteristics (how a person uses a specific service, from what device, by what clicking sequence,…) are currently only to be used as additional risk data for fraud detection (monitoring tool) and therefore a means for risk reduction (not for authentication). As such they are useful in the context of a risk based authentication model but cannot currently be recognised as an authentication factor on their own. It is also important to note that applicable privacy legislation should be respected when using behaviour-based elements. In any case, the possible use of behaviour-based characteristics should be left to the discretion of the ASPSP which at all times shall perform a SCA. It should neither be made mandatory nor forbidden by the EBA RTS. Behaviour based characteristics could possibly be replayed or copied or simulated by an impersonator, after studying a person for a while. They should therefore be used in combination with many other characteristics towards detecting abnormal constellations involving the transaction, its initiator and the client device used by the latter. An obvious pre-condition for the use of such elements is a PSU activity history in a given payment instrument that is significant enough to provide the means to identify such behaviour patterns. This precludes the use of this method for new users of a given instrument. In addition there is an absolute need for an adequate infrastructure that allows the online detailed monitoring of user activity, allowing for a real-time comparison between in-session activity and pre-saved patterns and, based on it, the capacity to raise the

	level of required authentication if any issue is detected that may suggest deviation from the pattern. Finally, it is worth noting that a PISP or AISP is an intermediary party between the PSU and the ASPSP. There is a potential risk that the interface between the PISP/AISP and the ASPSP will result in the loss of information that is required for a proper transaction risk analysis (e.g. IP address of the system/device used by the PSU).
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)?	
Response:	The actual challenge with respect to SCA is the sole control and possession by the PSU of the authentication factor rather than the independence of these factors. To comply with the "independence" as specified by PSD2 in the sense that "the breach of one element does not compromise the reliability of the other", the main challenge is how to preserve reliability in the event of a client device breach. There are challenges since the independence of the authentication elements used is never ensured. Indeed the PSU decides which device to use, for example its mobile device which intrinsically does not ensure independence. On the other hand there is a clear and strong market need for allowing a single device to deliver strong customer authentication, specifically from the perspective of user-friendliness. It is important to find the right balance between user experience and security. The issue of the independence of authentication elements is of course raised not only between the various elements themselves but also with regard to the use of a given element on a given device type or transaction context. The most commonly referred issue in this respect is the use of SMS One Time Passwords (OTPs) or App tokens on mobile banking devices, where should the device be compromised via a dedicated type of malware, OTPs could be tampered with, deviated or hidden, according to the attack vector. This sort of concern, that may occur in different types of devices or application contexts, does not immediately render useless the use of a given authentication method on a specific type of device, but may impose additional authentication methods under circumstances where the detected transaction risk patterns may be higher or where the combined infrastructure of hardware and software may present frailties that can be used in the context of fraud attempts. The use of non-physical possession elements (e.g. behaviour based characteristics) should be subject to this concern, as the compromise of a given device may provide the attacking hacker with the means to try to reproduce and/or simulate the previously referred "fingerprint" and, in that way, try to impersonate the PSU. Again, the use of complementary authentication methods, in circumstances where detected risk patterns rise above predefined critical thresholds, is the preferred manner to limit risk and ensure optimal transaction security levels at all times.

	It should be recognised that in recent years mitigating measures have been implemented on mobile devices which should be helpful towards guaranteeing the independence of two factors including for instance logical channel separation. The challenge will be that EBA should draft a set of requirements for implementing SCA within one physical device that is both secure enough and feasible. The existence and availability of mechanisms to block the use of the authentication elements in case the PSU loses control is crucial. Moreover, the ASPSP will have to compensate the lack of independence of the authentication elements on a mobile device with adequate fraud management. This fraud management will require detailed information of the associated payment information, used device and context usage.
5. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?	
Response:	Dynamic linking in the context of strong authentication must be assured on a trusted device, with trusted user interfaces (display and key pad or ok button). However this is currently not available on personal computers and partly available but not leveraged on mobile phones. The concept of dynamic linking should be clarified by EBA in the RTS, establishing some general criteria on dynamic codes. Nevertheless, it is fundamental to avoid the prescription of a specific solution or being too specific in the way dynamic codes are to be calculated, since meeting those requirements would be a challenge for PSPs. The criteria to be established should not hinder the ability of (European) PSPs to make use of international standards commonly accepted or existing business models (e.g., 3DSecure, recurring payments,…) Dynamic linking requires a trusted environment for either verifying or computing this linking. As long as mobile phones do not provide such a trusted environment (trusted hardware integration of their OS), secure dynamic linking can only be achieved through disconnected or securely shielded visualisation or generating tokens. The stipulations of Article 97(2) seem to impose that whenever used in the context of "electronic remote payment transactions" strong authentication factors must include "elements which dynamically link the transaction to a specific amount and a specific payee." This is of course not applicable to other uses of strong authentication, including those discussed when answering to Question 1 where payment data is not available, but risk factors are involved. A stringent interpretation of this notion would likely impose the need for differentiated strong authentication procedures for these

	two situations, something that seems very undesirable from the user experience/usability standpoint and also for the increased complexity of the solutions to be implemented and made available to PSUs. Various solutions have been used for several years now that link transaction data to authorisation codes in a manner that seems to respect the concept described in Article 97(2). That seems to be the case of SMS OTPs where the code is provided within a message where transaction data is also included. Other solutions involve dedicated physical devices, such as security tokens where transaction data is also added in the process of authorisation code generation. These, however, will probably suffer from the same problem mentioned before, as they seem more adapted to use in the context of payments rather than other types of transaction. Also, they often present logistics issues and have a negative impact on the user experience and ease of use, which may lead to bad security practices or to clients simply abandoning the channel. Seen from a strict perspective, the stipulations of Article 97(2) would even preclude the use of physical tokens where transaction data is not used in the generation of the code, such as those involving time-synchronised one-time passwords, which obviously guarantee a very high level of security in the context of most attack vectors currently experienced in the payment instrument environment. Going back to EBA's understanding of the main purpose of the dynamic linking requirement, the EPC opines that a solution that best protects PSUs and transactions while reducing negative impact on user experience, involves a balanced, proportionate and progressive authentication method portfolio, where strong authentication with dynamic linking is used for higher risk transactions and other strong authentication methods that do not involve this requirement are used in lower-risk situations. Naturally the general exceptions already considered in the new legislation for "high-confidence" situations where strong authentication is not mandatory still apply, and would in fact be a relevant part of this authentication method portfolio. Another challenge with respect to dynamic linking is for instance when the mobile payment service provider differs from the issuer of the authentication mechanisms (e.g. wallet provider).
6. In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?	
Response:	Subject to testing solutions that may fulfil both the objective of independence and dynamic linking against specific RTS the following may be considered: • Disconnected or securely shielded connected crypto hardware tokens used for the secure generation of dynamic signatures, as specified e.g. by CAP (chip authentication program) or for the secure visualisation of payment verification messages with approval codes.

	• Mobile OS integrations that leverage the trust zone concept for a secure OS integration and an on-board security module. • BankID (e.g., in Scandinavian countries). • Mobile app OTP generators. • Tokenisation.

2. The exemptions to the application of strong customer authentication (section 4.2)

General comments
With voice over IP commonly available on electronic platforms, it appears inconsistent to cite telephone orders as an example of a payment transaction initiated with a modality other than the use of electronic platforms or devices (cfr. 37). Definition of "trusted beneficiary" in 42.B. is too narrow. A previously established whitelist could also be made by the ASPSP e.g. including public administrations, utilities, etc. There seems to be an inconsistency with regard to the coverage of physical mail or telephone between 27iii, 43 and PSD2 (Article 4(6)). It is unclear who would perform the transaction risk analysis to determine whether or not a transaction constitutes a low risk transaction (cfr. 42 D).

7. Do you consider the clarifications suggested regarding the potential exemptions to strong customer authentication, to be useful?	
Response:	Clarifications are considered as useful examples but they should not be interpreted as an exhaustive list. It is to be noted that option (42.) D actually covers all the other options, since it allows for risk based exemptions that would presumably indicate acceptable risks for exemptions A, B, C and E. The EPC would therefore argue to base all exemptions on D, a risk analysis that results in a sufficiently low risk, which is in line with the principle of a risk-based approach. Therefore it is considered appropriate to define "risk-related thresholds" per specific service rather than an exhaustive list of exemptions related to specific transactions.
8. Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical	

standards?	
Response:	Another factor to be included is transfers between accounts for which the PSU has received prior authorisation from the effective account holder. This means that 42.C. appears to be too restrictive. Also 42.E. is relevant in relation to data protection and AIS.
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?	
Response:	The EBA should ensure that at broad level the following criteria are covered: • Consumer device level (device type, OS/browser, malware (not) present, rooted / jailbroken, device identification, etc.). • Connection level (direct / indirect, IP-address, IP GeoLocation, ISP, etc.). • Application level (language of the application, etc.). • Payer level (profiling, user interaction profiling, click-path profiling, etc.). • Transactional level (history, beneficiary account, amount, country, urgent/non-urgent payment, etc.). • Payee or beneficiary level (profiling). • Big data (data related to fraud / threat environment, customer claims). In addition, the criteria for this transaction risk-analysis should be principle-based. It is up to each type of PSP (ASPSP included) to decide on the exact capabilities of the fraud detection based on its own risk analysis and appetite. A PISP or AISP is an intermediary party between the PSU and the ASPSP. There is a potential risk that the interface between the PISP/AISP and the ASPSP will result in the loss of information that is required for a proper transaction risk analysis (e.g. IP address of the system/device used by the PSU).

3. The protection of the payment service users' personalised security credentials (section 4.3)

General comments
51.E. is not complete since it omits the last words of PSD2 Article 66.3(b): "ensure that… they are transmitted by the payment initiation service provider through safe and efficient channels". How to ensure this safe channel? Through encryption? 52.ii. "all communication channels (…) need to be resistant to tampering and unauthorised access". The EPC wishes to remark that this would be almost impossible to achieve. Standard (secure) protocols such as SSL1/2/3 and TLS1.0/1,2 were considered to be secure until new vulnerabilities were found. Such a requirement in the RTS would be too strongly formulated. Requirements for the resilience for tampering and unauthorised access should be formulated on messages and application protocols, not on the communication channels.

10. Do you consider the clarification suggested regarding the protection of users personalised security credentials to be useful?	
Response:	EBA's clarification seems to be appropriate but needs to be placed in the context of a consistent PSC level of assurance with regard to sole control. In addition, the RTS should clarify that the PSC of the PSU should never be exposed to anyone (with the exception of the user and the issuer of the personalised credentials), whereas the authentication codes which could potentially be exposed to a PISP should be authentication codes bound to a specific payee and specific amount, so that the exposure constitutes no risk for the PSU, irrespective of the fact whether these authentication codes are exposed to the right or the wrong intermediary. Note that SCA as defined in Article 4(30) PSD2 does not at all protect customers from the latter risk. In other words, a TPP should never be allowed to use the user ID/password solution, as it will be very difficult in that case to safeguard that the personalised security credentials are only used once. There are already technical solutions in place (e.g. OAuth[1], 3DSecure) that ensure that the customer does not need to share the PSC with AIS/PIS providers. In addition, the clarification does not address the issue of phishing (as mentioned in 51.D.). Phishing can be prevented if the use of PSCs is limited to secure environments that are recognisable by the PSU as being trusted environments (to limit/prevent phishing risks). One of the most effective anti-phishing measures is education of the PSU about where to enter his PSCs and how to

[1] OAuth: See http://oauth.net/2/

	recognise these as trusted environments. If the PSU is accustomed to entering their PSCs in many different environments (at many different TPPs) it becomes difficult to recognise a phishing-attempt by a rogue TPP, and it will be impossible to educate the PSU about how to recognise the trusted environments.
11. What other risks with regard to the protection of users' personalised security credentials do you identify?	
Response:	Generally, the threat landscape is evolving very fast. Currently, other risks identified include: • Dependence from third parties and third-party software (related to the PSU's ability to easily and naturally preserve sole control at a consistent PSC level of assurance). • Credential lifecycle (even without storing PSC at a PISP/AISP, these will always transit over the infrastructure of that PISP/AISP. It is therefore impossible to guarantee that only the user and issuer can access them). • Repudiation risks. • How can the PSU identify that the TPP is the correct one in an environment where a large portion of successful fraud attempts are the result of social engineering schemes or rely substantially on PSU unawareness? In a context where a significant number of PISPs and AISPs may appear, the need to provide the PSUs and ASPSPs with reliable information concerning the authenticity of these services and of application/sites that supposedly belong to them, is a key factor so that no attack vector can effectively exploit the possibility of someone impersonating an authentic player or presenting itself as a PISP/AISP while in fact, using such a procedure with the purpose of capturing the PSUs PSC in an apparently legitimate process.
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?	
Response:	Innovative solutions for credential issuers include: • Customer biometrics. • Leverage of national electronic identity systems and bank IDs related to remote customer enrolment. • Physical card entry in an ATM where a unique code (possibly in the format of a QR-code) is generated and used to enrol a

	device or a profile on a device. • Credential generation in on-board TPMs on client devices with a trusted OS integration. • Mobile device binding (secure activation of an app for use by only one PSU on only one device).
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 unauthorised access?	
Response:	No, there are no available alternatives. Any technical component should be certified and evaluated by third parties in analogy to already existing processes like EMVCo, PCI, etc. However, it is assumed that the existing certification rules are taken into account for setting concrete requirements in the RTS. Given the fact that organisations are sometimes subject to a wide range of security related certification programs such as PCI DSS, PCI PIN and EMVCo, resulting in the repetitive evaluations and auditing of the same systems and processes, some rationalisation in this field would be appreciated, if possible. It would be beneficial to implement a framework building upon present day programs in order to avoid inefficiencies. All manufacturers and service providers including TPPs should comply with these certifications/evaluations.
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?	
Response:	Major risks are with the PSU, who may be unable to control the security of their devices (PC or mobile) or to preserve proper sole control over its credentials, if not enabled through simple and natural behaviour rules. Advanced social engineering attacks that are not inherently excluded or rendered ineffective though the authentication technology and its integration are likely to succeed. Likewise, if PSUs get trained to hand out their credentials or thereof derived codes in whatever form (plain or encrypted) to any third party, other than the ASPSP which issued these credentials, the security and trust in the whole underlying payment system will eventually be at risk. The transmission of the PSC's between the PSU and ASPSP or between the ASPSP and TPP. When a TPP is acting on behalf of the PSU or a software element is initiating a payment in a device without full control by the PSU the risk of impersonation (MITM - Man In The Middle) and unauthorised access to personalised security credentials increases.

	Replay protection via protection of the channel or dynamic credentials. Cloud-based computing could also represent a concentration risk whereby it offers an attractive target for hackers to stage a large attack for stealing PSU credentials or creating fake ones. Cross-contamination. For instance if credentials can be used across the banking industry and governmental services this may be opening many forms of data leakage and possible ways to access critical information. It is therefore important that third parties only get access to the necessary information, and, preferably, that the PSU notifies the ASPSP about which service(s) a specific third party should be allowed to access on their behalf. In general, the more parties or entities play a significant role in the payment chain (e.g. processing sensitive payment data), the more places there are where risks are introduced.

4. Considerations prior to developing the requirements on common and secure open standards of communication (section 4.4)

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?	
Response:	Clarifications are deemed mostly comprehensive and suitable but standardisation is vital. Additional topics of major relevance are: • The way AIS and PIS providers authenticate towards PSUs, as this is crucial for the PSUs to preserve sole control over their PSCs, by adhering to easy applicable rules when it comes to exposing only what is allowed to whom it is allowed. • The way PSUs authenticate towards their ASPSPs, when AIS or PIS providers are involved in the service provisioning process, as it is key, pursuant to the PSD2, that AISPs and PISPs have no access to the credentials issued by an ASPSP; effectively meaning that the AISP or PISP have no way to impersonate the PSU by exploiting its credentials or thereof derived codes for any other means than what they were explicitly generated for by the PSU. • TPPIIs (Trusted Party Payment Instrument Issuers) (e.g., Card or Wallet providers). • An AISP/PISP should not only forward transaction-related information to the ASPSP, but also information about the process itself (time of payment process, etc.) and consumer device (device footprint, IP address, etc.), depending on the risk

	profile of the transaction. This kind of information can be used by the ASPSP in its risk analysis and fraud monitoring process. • Access may be restricted or blocked in case of any abnormal access by frequency or volume (e.g., denial of service attacks).
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?	
Response:	The following topics need to be addressed: • Specification of generic request, response and authentication messages, irrespective of the underlying communication protocol; • Specification of at least one appropriate communication protocol, to be supported by all registered participants; • Specification of a certification authority that supports easy and up-to-date authentication of authorised payment service providers (e.g. through the issuing of attribute certificates); • Governance (management of liabilities and claims…). In a nutshell, simplicity is essential here but on the other hand flexibility must remain an option for established national preferences to co-exist.
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?	
Response:	With respect to the interface between AISP/PISP and ASPSP, established European corporate banking interfaces could be leveraged, towards a standardised uploading and downloading of single transaction or account data by AISPs and PISPs. As most of them require the client side to work with PKI certificates, this could match with the normal server-based access from AIS and PIS provider environments. OAuth 2.0 / W3C (if available) / SEPAmail standards should be taken into consideration.
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)?	
Response:	Preferably, the RTS should refer to commonly accepted international standards already in use and establish clear criteria that allow the adoption of other standards that could potentially be developed in the future instead of only devising a European solution. There is no doubt that these will be evolving standards, not only for innovative solutions that will certainly appear, but also for what is known at this time. In areas where maturity levels are high (ranging from EMV to TLS[2] standards) standards are ever evolving in response to technological improvements and to new threats. In this highly dynamic arena of payment services on the internet it is crucial to have swift responses adapting to new scenarios. Not doing so will be detrimental to the objective of the PSD2 in what relates to the security of electronic payments in order to "ensure the protection of users and the development of a sound environment for e- and m-commerce".

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

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.	
Response:	As the e-IDAS Regulation specifies principles and requirements regarding identity and authentication levels, it represents an opportunity for European customers to benefit from harmonised principles of identification and authentication all over Europe. However, the e-IDAS Regulation has been developed to secure an authentication of an identity and not the authenticity and integrity of a payment transaction. The considerations of dynamic linking and behaviour based fraud management are not in the scope of e-IDAS. e-IDAS deals with PSC levels of assurance for sole control. PSC levels of assurance will have to be specified for customers and service providers also in the context of PSD2. Alignment with the assurance levels defined by e-IDAS is strongly encouraged for

[2] TLS: Transport Layer Security

	simplicity, intelligibility and reusability reasons. More in particular, online customer acquisition (based on national identification/authentication systems or other identity trust providers), where there is a risk for customer impersonation that could result in KYC-related risks (e.g., money laundering) (cfr. e-IDAS). However, enrolment processes will have to be reviewed in view of their applicability to PSD2 and in view of the fact that e-IDAS credentials may generally be issued by non-PSD2 regulated third parties, although this does not exclude PSPs from taking on this role. Furthermore, regarding mutual server authentication processes, e-IDAS could be used for the server seal at an appropriate security level. In any case, the dialogue and close collaboration on these matters between the EU institutions and the public and private sectors will be crucial in order to devise secure and effective solutions into that context and more broadly as part of the Digital Single Market. Indeed, to fully benefit from cross-country and cross-sector use of eID and eTS (electronic Trust Services) there is a need for a careful review and clarification of supervision and liability settings, especially in circumstances where both the e-IDAS Regulation and the PSD2 would apply.
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.	
Response:	Qualified trust services with a proper level of security assurance for sole control are conceivable to be used as PSCs for AISPs, PISPs and ASPSPs. Alternatively, also certificates from trusted commercial Certification Authorities (CAs) with a secure registration process could be allowed for this purpose, if in line with the PSC level of assurance for PSPs, yet to be specified. Irrespective of that, a dedicated CA must be established which issues trusted attribute certificates for a proper cross-border identification of all PSPs, registered and regulated according to PSD2. However, the qualified trust services involved should be subject to the same liabilities as the other participants in the payment value chain.